CHAPTER

36

High-Rise Security*

Geoff Craighead, CPP

INTRODUCTION

An office building is a “structure designed for the conduct of business, generally divided into individual offices and offering space for rent or lease.”[1] The types of office buildings addressed in this chapter are those that have one or more tenants conducting various types of commercial business and may include public service offices (however, they do not comprise tenants such as courthouses and police holding cells). Depending on the country, state, or city in which such buildings are situated, they have to be operated according to specific industry-related guidelines and standards, many of which are government mandated.

Office buildings usually “include parking facilities which may be open, enclosed, above- or below-ground, and often directly beneath or adjacent to the [office building] itself. These arrangements may require special types of fire protection, and the building codes may require fire separations.”[2]

To systematically examine the security and fire life safety of office buildings, this chapter addresses the following areas: occupancy characteristics; assets, threats, vulnerabilities, and countermeasures; security programs; and emergency planning.

OCCUPANCY CHARACTERISTICS

“The types of building tenancy and the pattern of use are important factors to consider when we plan and carry out a security [and fire life safety] program. A building can be (1) single-tenant/single-use, (2) single-tenant/multiple-use, (3) multiple-tenant/single-use, or (4) multiple-tenant/multiple-use.”[3]

- A *single-tenant/single-use* building is occupied by one particular tenant and is used solely for one type of business; for example, a bank building where the business of that bank alone is conducted.
- A *single-tenant/multiple-use* building, however, is occupied by one particular tenant who uses the building not only for one type of business but also for other purposes. An example would be a bank building that has parking facilities, restaurants, a cafeteria, or retail outlets open to the public.
- A *multiple-tenant/single-use* building is occupied by more than one tenant, each of whom uses the building to conduct a similar type of business; for example, a medical office building where tenants conduct medical business.
- A *multiple-tenant/multiple-use* building is occupied by more than one tenant, each of whom conducts business not necessarily related to the other businesses. An example would be a commercial office building that has law firms, public utilities or agencies, management consultants, financial institutions, retail outlets, and public restaurants.

Office buildings usually have a higher concentration of occupants during normal business hours (i.e., Monday to Friday, during daytime hours), when the building or property management staff tend to be on duty. After hours (i.e., Monday to Friday, early evening until the next morning, and on weekends and holidays), most buildings (except major facilities, including mega high-rise buildings) have fewer engineers (if any), security personnel, elevator technicians, and other support staff on duty; however, there is usually a higher concentration of janitorial and cleaning staff from early evening (Monday to Friday) until the early hours of the next morning, because cleaning operations are generally focused during the hours when most tenants are not present.

Generally speaking, office buildings are managed by one group; this will consist of a building or property manager and administrative staff, plus support staff such as in-house or contract engineers, security personnel, janitors and cleaners, elevator technicians, landscaping staff, and other vendors associated with

* Originally from Craighead G. High-rise security and fire life safety. Boston, MA: Butterworth-Heinemann; 2009. Updated by the editor, Elsevier, 2011.

building operations. The actual numbers of staff will vary according to the size of the building, the complexity of its operations, and the security needs of each individual facility.

Building or property management staff tends to be on duty during normal business hours (i.e., Monday to Friday, during daytime hours). After hours, such staff can be contacted using various means of communication that include telephones, pagers, e-mail, and text messaging. Some buildings designate an on-duty manager to handle after-hours calls relating to building operations.

ASSETS, THREATS, VULNERABILITIES, AND COUNTERMEASURES

A risk assessment is an important tool for developing an appropriate security and fire life safety program for an office building.

> *[A]risk assessment analyzes the threat, asset value, and vulnerability to ascertain the level of risk for each critical asset against each applicable threat. Inherent in this is the likelihood or probability of the threat occurring and the consequences of the occurrence. Thus, a very high likelihood of occurrence with very small consequences may require simple low cost[,] mitigation measures [countermeasures], but a very low likelihood of occurrence with very grave consequences may require more costly and complex mitigation measures. The risk assessment should provide a relative risk profile. High-risk combinations of assets against associated threats, with identified vulnerability, allow prioritization of resources to implement mitigation measures.*[4]

Key steps in the process involve examining the assets, the threats against the assets, the vulnerabilities of the assets, and the countermeasures or mitigation measures that can be used to address identified vulnerabilities of the assets (within the confines of risk management). These areas are now examined for office buildings.

Assets

Tangible assets in office buildings include the lives of tenants, visitors, contractors, vendors, and the office building staff; tenant property; and the building itself, its fittings, and its equipment. Building equipment includes electrical, water, gas, mechanical, heating, ventilating, air conditioning, lighting, elevator, escalator, communication, security, and life safety systems. In addition, there are other types of assets that may include telephones, computers, printers, typewriters, fax machines, photocopiers, audio-visual equipment, and general-use items (coffee machines, vending machines, refrigerators, microwaves, ovens, and furniture) and sometimes antiques and works of art, cash, and negotiable instruments, and vehicles parked in a building's parking garage. In addition, there may be assets in cafeterias, restaurants, retail shops, newsstands, copy/print services, and other common area facilities.

Intangible assets include the livelihood of building tenants, visitors, contractors, vendors, and office building staff; intellectual property and information stored in paper files, reference books, microfilm, and within computer systems and peripherals; and the reputation and status of the office building and its tenants.

Threats

The types of security and fire life safety threats to office building assets include the following:

- **Security threats to people**: Assault, assault and battery, kidnapping, manslaughter, mayhem, murder, robbery, sex offenses (including rape, sexual harassment, and lewd behavior), and stalking.
- **Security threats to property and information**: Aberrant behavior, arson, burglary, cyber-attack, disorderly conduct, espionage, larceny, sabotage, theft, trespass, and vandalism. In addition, there may be the disruption of building utilities such as water, electrical power, natural gas, sewer, heating, ventilation, and air conditioning (HVAC), telecommunications, security, and life safety systems. Some security threats may involve terrorism.
- **Security threats to people and property**: Bombs, chemical and biological weapons, riots and civil disturbances, fires and fire alarms, hazardous materials, natural disasters, and nuclear attack.
- **Life safety threats**: Aircraft collisions; bombs and bomb threats; daredevils, protestors, and suicides; elevator and escalator incidents; fires and fire alarms; hazardous materials, chemical and biological weapons, and nuclear attack; kidnappings and hostage situations; labor disputes, demonstrations, and civil disorder; medical emergencies; natural disasters (earthquakes, tsunamis, volcanoes, heat waves, storms, and floods and landslides); contractible diseases (pandemic influenza, severe acute respiratory syndrome, and tuberculosis); power failures; slip-and-falls; stalking and workplace violence; traffic accidents; and water leaks.

Notable Incidents. Some notable incidents[5] that have occurred in high-rise office buildings are shown in Table 36-1.

Fire Risk in Office Buildings. Fire is a constant risk in high-rise office buildings. In discussing fire risk (here, "risk" refers solely to the risk of having a reported fire), it is helpful to analyze fire incident data for the four property classes — office buildings, hotels and motels, apartment buildings, and hospitals (and other facilities that care for the sick) — that account for the majority of high-rise building fires.[6] Even though this data pertains only to the United States, it is worth considering because

TABLE 36-1 Notable High-Rise Office Building Incidents

Date	Building	Incident	Persons Killed/ Injured
February 1, 1974	Joelma Building, São Paulo, Brazil	Fire	179 killed, 300 injured (greatest loss of life in an office building fire)
May 4, 1988	First Interstate Bank Building, Los Angeles, California	Fire	1 building engineer killed, 40 injured
June 30, 1989	Peachtree 25th Building, Atlanta, Georgia	Fire	5 killed, 26 injured (including 6 firefighters)
February 23, 1991	One Meridian Plaza, Philadelphia, Pennsylvania	Fire	3 firefighters killed
February 26, 1993	New York World Trade Center, New York	Truck bomb	6 killed, 1042 injured
April 24, 1993	Bishopsgate area of London's financial center, U.K.	Truck bomb	1 killed, 44 injured
July 1, 1993	101 California, San Francisco, California	Shooting	8 killed, 6 injured, gunman killed himself
April 19, 1995	Alfred P. Murrah Building, Oklahoma City, Oklahoma	Truck bomb	167 killed, 782 injured
November 20, 1996	Garley Office Building, Hong Kong	Fire	40 killed (including 1 firefighter), 81 injured
July 29, 1999	Several buildings, Atlanta, Georgia	Shooting	9 killed, 13 injured, gunman shot himself
September 11, 2001	New York World Trade Center, New York	Aircraft collision	2749 killed, thousands injured
March 11, 2002	Rembrandt Tower, Amsterdam, Holland	Hostage	18 held hostage (none hurt), gunman shot himself
October 17, 2003	69 West Washington, Chicago, Illinois	Fire	6 killed
November 20, 2003	HSBC Bank AS and British Embassy, Istanbul, Turkey	2 truck bombs	30 killed, 400 wounded
October 15, 2004	Parque Central, Caracas, Venezuela	Fire	Building unoccupied apart from several security staff who evacuated safely
February 12, 2005	Windsor Building, Madrid, Spain	Fire	Building unoccupied apart from several security staff, was demolished due to extensive fire damage
December 8, 2006	Citigroup Center, Chicago, Illinois	Shooting	3 occupants killed, gunman shot himself

it includes the types of commercial buildings that are addressed in this book (namely, office, hotel, residential and apartment, and mixed-use buildings).

A study by Dr. John Hall, Jr., of the National Fire Protection Association's (NFPA) Fire Analysis and Research Division, using statistics from the U.S. Fire Administration's National Fire Incident Reporting System (NFIRS), stated that from 1987 to 1991, office buildings, hotels and motels, apartment buildings, and facilities that care for the sick averaged 13,800 high-rise building fires per year and associated annual losses of 74 civilian deaths, nearly 720 civilian injuries, and $79 million in direct property damage. However, "most high-rise building fires and associated losses occur in apartment buildings."[7] Hall added that for this period:

- Only a small share of high-rise building fires spread beyond the room of origin, let alone the floor of origin.
- In high-rise buildings (office buildings and hotels and motels), electrical distribution system fires rank first in causes of fire-related property damage.[8]

The most recent published study by Hall shows that "in 2002,[9] high-rise buildings in these four property classes combined had 7,300 reported structure fires and associated losses of 15 civilian deaths, 300 civilian injuries, and $26 million in direct property damage."[10] He concluded that "these statistics generally show a declining fire problem over the nearly two decades covered"[11] and, similar to his previous findings, "most high-rise building fires and associated losses occur in apartment buildings."[12] However, Hall did caution that, due to a number of factors (one being lower participation in national fire incident reporting in recent years[13]), "the patterns shown in data available so far should be given limited weight."[14]

Vulnerabilities

Weaknesses that can make an asset (in this case, an office building and its operations) susceptible to loss or damage[15] will largely depend on the building itself and the nature of its operations. A vulnerability assessment is required to "evaluate the potential vulnerability of the critical assets against a broad range of identified threats/hazards."[16]

Countermeasures

Mitigation measures to counteract identified vulnerabilities of an asset to a threat may consist of security systems and equipment, fire life safety systems and equipment, security personnel, security policies and procedures (see the next section, Security Programs), and emergency management (see section, Emergency Planning). These countermeasures need to be looked at in terms of security design. "Security design involves the systematic integration of design, technology, and operation for the protection of three critical assets — people, information, and property…. The process of designing security into architecture is known as crime prevention through environmental design (CPTED)."[17] As mentioned previously, the key to selecting appropriate countermeasures for a particular facility is for a risk assessment to be conducted.

Because fire is a risk in high-rise buildings, the following is noted regarding their fire protection features: office buildings that have properly designed, installed, operated, tested, and maintained automatic fire detection and suppression systems and other fire protection features — automatic closing fire doors for compartmentation and maintenance of the integrity of occupant escape routes and automatic smoke control systems to restrict the spread of smoke — do have the necessary early warning systems to quickly detect fires and warn occupants (including tenants and visitors) of their presence, as well as the necessary automated sprinkler systems to quickly extinguish a fire in its early stages. One of the key issues here is the presence or absence of sprinklers.

In the study mentioned in the previous section called Threats, Hall commented on fire protection in high-rise buildings by stating that

> *In several instances, the value of these fire protection features [i.e., automatic extinguishing systems (primarily sprinklers), fire detection equipment, and fire-resistive construction] may be seen clearly in a statistical analysis of 1994–1998 loss per fire averages, with and without the protection. For high-rise buildings, automatic extinguishing systems are associated with a reduction of at least 88% in the rate of deaths per 1,000 fires for each of the three property classes (excluding office buildings, which had no deaths recorded in NFIRS [National Fire Incident Reporting System] in high-rise buildings) and at least 44% in the average dollar loss per fire for each of the four property classes….*
>
> *Automatic extinguishing systems and fire detection equipment and the compartmentation features associated with fire-resistive construction all contribute to fire protection by helping to keep fires small, with extinguishing and construction doing so directly and detection doing so by providing early warning that can lead to earlier manual suppression.*[18]

SECURITY PROGRAMS

Security programs for office buildings and for individual tenants involve policies, rules and regulations, and procedures designed "to prevent unauthorized persons from entering, to prevent the unauthorized removal of property, and to prevent crime, violence, and other disruptive behavior."[19] Security's overall purpose is to protect life and property.

Building Access Control

There are many different people who may, at any one time, wish to enter an office building.They include building owners and management staff, building contractors (such as engineering, maintenance, security, janitorial, and parking personnel and elevator technicians), tenants (and the employees working for them), visitors, salespersons, trades people (including construction workers, electricians, plumbers, carpenters, gardeners, telecommunications repair persons, persons replenishing vending machines, and others who service equipment within the building), building inspectors, couriers, delivery persons, solicitors (a person who approaches building occupants with the intent to sell something, to ask for business for a company, to request charitable contributions, or to obtain magazine subscriptions. This definition would include people who beg or panhandle for money or food), sightseers, people who are lost, vagrants or homeless people, mentally disturbed individuals, vandals, suicidal persons, protestors, and daredevils. There may also be others who try to enter a building — or an individual tenant space — with the sole aim of committing a crime.

Such persons may include a "building or office creeper," who may enter a building that does not have strict access control measures. For example, late in the afternoon, dressed in conservative business attire, the creeper might confidently enter through the main lobby and nonchalantly pass by building security staff. Taking an elevator to an upper floor, this "businessperson" enters a common area restroom and quietly sits in a cubicle until the tenants on the floor are about to close business for the day. He or she then exits the restroom and systematically walks the corridors checking doors to see if they have been secured. On finding one unlocked, the creeper enters the tenant space and proceeds through it looking for laptop computers, personal data assistants, mobile telephones, cash, checks, credit cards, and other items that can be easily placed in a jacket or a briefcase. On being challenged in one suite by building janitorial staff, a tenant business card (which moments before was lifted from an executive's desk) is politely presented with the statement of gratitude, "I'm so glad to see that even janitorial staff in our building are so security conscious!" After 15 minutes of work, the creeper descends to the lobby in a passenger elevator and warmly waves to the security staff as he or she exits the building. The advent of mobile phones has made it possible for such persons to operate in pairs.

To deter this type of activity, tenants should ensure that all perimeter doors not supervised by staff be kept locked; employees should be instructed to not allow unknown persons to tailgate or piggyback into their offices, to challenge unknown persons encountered inside their offices (even if they are wearing a service uniform and look like a delivery person, janitor, or maintenance worker), and to not leave business and personal items unattended.

It is primarily the building owner and manager who determine the access control measures for this wide spectrum of persons. These measures aim to screen out unwanted persons or intruders and at the same time provide a minimum of inconvenience to legitimate building users. When a security program is designed, occupancy characteristics such as the type of building tenancy, its pattern of use, and the time and day (normal business hours or after hours, weekends, and holidays) need to be considered. "The dilemma that office building owners and managers face is to keep the building secure, while allowing entry to legitimate users and exit under emergency conditions. While authorized personnel should be allowed to come and go with relative ease, unauthorized individuals require restricted access."[20] Varying degrees of access control can be achieved using security staff — in some office buildings they are known as security officers, security guards, or other titles that differ according to their respective duties and responsibilities — or nonuniformed receptionists and customer service staff, along with various other security measures.

As explained earlier in this chapter, an office building can be single-tenant/single-use, single-tenant/multiple-use, multiple-tenant/single-use, or multiple-tenant/multiple-use. A single-tenant/single-use building is much more conducive to strict access control of employees and members of the public: standard security rules and procedures can be communicated and enforced more easily with employees of one tenant only. "Access control may be tight and involve a badging system for regular employees and a careful monitoring of visitors through direct observation, or video displays and other devices."[21] Implementation of strict access control for a multiple-tenant/multiple-use building, however, is more difficult because each tenant may have different expectations of the degree of security the building should have. Before the September 11, 2001, destruction of the New York World Trade Center, access controls in many multiple-tenant commercial office buildings were generally loose during normal business hours, Monday to Friday, and tightened up after hours. Since that incident, many buildings have implemented strict access controls 24 hours per day, 7 days per week.

Building access controls include vehicle access to parking lots, garages, and loading dock/shipping and receiving areas; pedestrian access to building lobbies, elevator lobbies, and passenger and freight/service elevators; and access routes to retail spaces, restaurants, promenades, mezzanines, atria, and maintenance areas. Measures for controlling access to these areas vary from site to site, depending on building management's policy, but generally incorporate some or all of those described in the following sections.

Vehicle Access to Parking Lots or Garages. Access to parking lots or garages may be manual or automatic using a variety of methods that include the following:

1. Entry at will. There are no controls on the entry of vehicles (apart from possible vehicle height, weight, and width restrictions at the point of entry).
2. A vehicle detector embedded in the roadway, which automatically opens an entry gate or raises a gate arm.
3. A parking attendant, a valet, or a security person stationed at the point of entry or at a remote location linked to the point of entry by an intercom or a closed-circuit television (CCTV) system and a key switch or a remote control device that opens an entry gate, raises a gate arm, or lowers a surface-mounted traffic barrier.
4. A ticket (imprinted with the date and time of entry) dispensed by a machine at the point of entry that when withdrawn from the control unit automatically opens an entry gate or raises a gate arm.
5. An electronic access card, an alphanumeric key pad, or a vehicle identification system such as a transponder that opens an entry gate, raises a gate arm, or lowers a surface-mounted traffic barrier.

When exiting a controlled-access parking lot or structure, the driver usually is required to submit to a similar procedure to that encountered on entry, make a monetary payment (sometimes using a pay-on-exit machine), or use a token. Many access control systems with entry and exit card readers incorporate an anti-passback feature. This prevents an access card from being used again to authorize entry of a second vehicle before the card has been used to authorize exit of the first vehicle.

Vehicle Access to Loading Dock/Shipping and Receiving Areas. Vehicles entering loading dock/shipping and receiving areas may do so at will and park at whatever loading bays or docks are available, or they may be permitted to enter and be directed to park in certain areas by a loading dock attendant who will then supervise subsequent loading or unloading. (Some buildings keep loading dock doors and gates closed between delivery and pick up of items. Also, docks that are normally unattended may have an intercom or buzzer system, possibly in conjunction with CCTV, to allow drivers to remotely summon building staff for assistance.)

Some higher security buildings require vehicles, particularly vans and trucks, and especially those that will proceed to underbuilding loading dock/shipping and receiving areas, to undergo an on-street visual inspection before being allowed to enter. (As a result of the events of September 11, 2001, some landmark high-risk office buildings deployed a mobile X-ray vehicle to screen such vehicles, including trucks, for explosives, prior to entry.)

For security purposes, the dock attendant normally will maintain a log or record of the vehicle license plate number, the driver's name and company, the time in, and the time out. Depending on building policy, vehicle keys may remain in the vehicle or be given to the dock attendant for safekeeping and to permit moving the vehicle if necessary.

The activity of drivers and delivery persons usually will be confined to the loading dock/shipping and receiving areas, unless they need to proceed to tenant areas for deliveries or pickups. For this reason, rest areas, toilet facilities, and pay phones often are provided in these areas. If drivers and delivery persons enter the building, they are usually required to notify the dock attendant of the specific building area they will be visiting and the approximate duration of their stay. They may also be issued special identification badges and be required to leave some form of personal identification (such as a driver's license) with the attendant. (Since September 11, 2001, many office buildings strictly control drivers and delivery persons entering loading dock/shipping and receiving areas. Again, some landmark facilities, due to the perceived risk of dangerous or illegal items being brought into the loading dock area, have installed walk-through metal detectors and pallet-size X-ray machines and have utilized portable, hand-held explosives trace detectors or explosive-detection trained dogs.) (See also the section Dangerous or Illicit Items.)

Pedestrian Access to Buildings. Pedestrians entering office buildings during normal business hours may simply enter at will and proceed to whatever area they desire, or they may be asked to submit to some form of credentialing process before they are permitted to enter the facility and proceed to interior locations. The process in place may vary according to the time (either normal business hours or after hours) and the day (either standard working days or weekends and holidays) that the access is requested.

Normal Business Hours

During normal business hours, access control for some office buildings and their common areas is relaxed and may solely rely on a security officer or receptionist trained to observe both incoming and outgoing pedestrian traffic. Persons who do not appear to belong in the business environment may be challenged with a simple "May I help you?" Specific questions can then determine the particulars; for example, whether the person is a tenant, is visiting a tenant (if so, which one?), is delivering or picking up items (if so, to whom? from whom?), or is servicing or inspecting equipment in the building (if so, where? at whose request?). These questions not only help screen out intruders with no legitimate reason for entering but also assist persons who need directions.

For other buildings, access control is stricter, relying on a variety of methods such as electronic access cards (which are presented to readers at building entrance doors, at lobby kiosks, on elevator bank walls, or inside elevator cars) and optical turnstiles. For tighter security applications, access control may even involve biometric devices or a combination of technologies for identity management. The degree of access control imposed by building policy determines the percentage of unwanted persons successfully screened out. "The security program should be designed just tight enough to screen out as many intruders as it takes to reduce problems to the level that can be accepted. This means that a useful security program will rarely screen out all intruders."[22] If all intruders were screened out, it may result in what could be considered by building management as unacceptable delays or inconvenience to the legitimate occupants and visitors.

The screening of visitors may be facilitated by establishing separate visitor centers and using visitor management software to expedite entry. The former allows visitors to be moved to a separate staging area for processing. The latter is a password-protected, Web-based management system that permits authorized users of the system to preregister visitors online before they arrive at a building. All relevant information about the visitor (such as name, company, person they will be visiting, time of visit, and any special instructions for handling the visitor) can be stored in a database and used to print out a visitor badge when the person is cleared for entry. This not only facilitates visitor handling but also records visitor traffic and could be used to track the attendance of vendors and contractors. Some systems even allow the visitor to self-register by scanning an identification document, such as a driver's license, through a verification machine.

Access control to building maintenance spaces — mechanical rooms and floors, air-conditioning rooms, telecommunications and utilities access points, elevator machine rooms, and janitorial closets — and areas under construction or renovation usually will be tight. Depending on building policy, persons accessing these areas may be logged in and out, required to wear special identification badges, given keys (although issuing keys to vendors or visitors can be a security risk) or an electronic access card to a particular area (if the card is not returned it can be immediately deactivated), or provided an escort. Some contractors servicing certain types of equipment in specific building areas may be permitted to install their own locking devices at access points leading to this equipment (see further comments in the section Key Points to Consider). Main electrical switchgear and power transformer rooms are usually deemed such a life safety risk that building personnel are not issued keys to these areas.

After Normal Business Hours

After normal business hours, access control to most office buildings and interior areas is usually strict. An obvious way to provide off-hours access to an office building would be to furnish keys to all building occupants or to those who need to enter the facility after hours. This approach, however, can have disastrous consequences proportional to the size of the building and the number of occupants. A heavy workload and costly expense can be created by lost keys, keys not returned by departing tenant employees, and the necessity of rekeying building entrances and reissuing keys to building key holders every time a key has gone astray. In addition, there may be the problem of the unauthorized duplication of keys. To avoid all these consequences, most office buildings never issue building access keys to tenants but rely on some way of verifying a person's right to enter the building. This verification may involve the following procedures.

Visual Recognition. Building security staff or a receptionist may verify on sight a person's right to enter. Several problems may result, however, from this form of verification. For example, someone who closely resembles a person authorized to enter may be admitted in error. Also, particularly if the building is large with a high population, it will be difficult for security staff or the receptionist to recognize all persons authorized to enter. If there is a change or substitution of the security staff or receptionist, the new person will not be familiar with the persons authorized to enter. This may result in the questioning of authorized persons who normally are never challenged and subsequent complaints to building management. Finally, if the security staff is distracted by another duty, an unauthorized person may gain entry without being observed.

Authorization Documents. A document (a letter, a memorandum, or an e-mail) listing those authorized for after-hours access may be provided in advance to security staff at the building entrance. Persons requesting access will identify themselves to building security staff. Security will compare their name (which should be confirmed by a driver's license or other photo identification) with the names listed in the document. In many buildings, tenants will provide management with a written request on their own stationery listing the names of the persons involved and the time after-hours access is permitted. Building security staff or the receptionist often will set up a file sorted alphabetically by tenant name, or by the last name of the person to be granted access, to minimize time spent searching for the appropriate authorization.

Building security staff must thoroughly check all documents authorizing access to ensure that the decision to grant access is valid. An unusual example illustrates the point. Building management of a major office building gave building security staff a memorandum to allow access of a pest control company to a specific tenant suite on a particular Friday night. The pest control company failed to appear on the night authorized but did arrive the following Monday evening. Building security staff did not thoroughly check the paperwork and permitted the pest control company to enter and carry out their work. The next business day, several of the tenant employees became ill from the lingering effects of the pest treatment. The reason for authorizing entry on Friday evening was to allow two days for any residual pesticide to dissipate. Permitting the work to occur on a Monday evening negated this precautionary safety measure.

Building Identification Cards, Passes, and Badges. A building identification card, a pass, or a badge is sometimes used to verify the bearer's identity and privilege to enter after hours. The identification means should be numbered sequentially, stating the person's name and the company's name, and should contain the person's signature, a color photograph, and in some instances an expiration date. It should be laminated for durability, and be tamper resistant (although this will not necessarily eliminate the potential for the plastic envelope being cut and the card, pass, or badge being modified and then re-laminated). The development of laser technology to create holograms (three-dimensional images) may lead to their future use for building identification cards, passes, or badges.

The credential can be presented by the bearer to security staff for entry to the building or used to verify identification within the building. However, if the card, pass, or badge is not thoroughly checked for details, this form of access control soon loses its effectiveness. Also, it must be retrieved from holders whose employment is finished, or else it could be used after the person no longer has a legitimate reason for gaining access to the building.

In case the card, pass, or badge is lost, it should not identify the building but can include text such as

IF FOUND, DROP IN ANY MAILBOX.

P.O. BOX NO. ___, CITY & STATE.
POSTAGE GUARANTEED.

Building Electronic Access Cards. Building electronic access cards can provide after-hours access by operating a building entry door. An intercom, a telephone, or a CCTV camera may also be situated at the point of entry. If there is a problem using the card, the person requesting access can use the intercom or telephone to communicate with on-site security staff or an off-site central monitoring station. If the person's right of entry is confirmed, the staff can grant access in person or remotely.

Once a person is inside a building lobby, his or her progress may be controlled using a variety of methods. These include electronic access cards presented to readers at lobby kiosks, on elevator bank walls or inside elevator cars, and to optical turnstiles; for higher security applications, the method may even involve biometric devices or a combination of technologies for identity management.

An access control system installed in passenger and freight/service elevator cars provides controlled access to building floors. Some systems can be programmed so that during certain time periods the elevator car will only respond to a particular floor if an authorized access card is used. The person will enter the elevator, insert, swipe, or bring the card into close proximity to the card reader, and select the desired floor by pressing the appropriate button on the floor selection panel. (Additionally, in high-traffic buildings that have elevator systems equipped with destination dispatch technology, access control systems may be incorporated with such technology. In the elevator lobby, the waiting passenger uses a touch screen or a keypad located on elevator bank walls or lobby kiosks to select the required destination floor and is also required to present a valid access card to a reader incorporated into the system; or a person uses an access card to pass through an optical turnstile that also controls access to the elevator banks. The elevator control system evaluates the data, dispatches an appropriate elevator car to the floor where the passenger is waiting, and directs the person to the appropriate car.)

Building access cards can feature the same data, tamper-resistive protection, and lost-card notice as identification cards, passes, and badges. However, for security reasons managers of some buildings prefer to have no information displayed on the card apart from its sequential number and, if used with an insertion or swipe-type card reader, an arrow depicting the correct way to insert or swipe the card. Then if a card is lost, there are no identifying marks to indicate where it may be used. An advantage of an electronic access card is that if the cardholder's employment ceases, a computer can be used to deactivate the card immediately, eliminating the need to retrieve the card.

Visitor Management Software. As previously explained, visitor management software is a password-protected, Web-based management system that permits authorized users of the system to preregister visitors online before they arrive at a building. All relevant information about the visitor (such as name, company, person they will be visiting, time of visit, and any special instructions for handling the visitor) can be stored in a database and used to print out a visitor badge when the visitor is cleared for entry (the value of visitor badges decreases if the visitor is allowed access to areas where occupants are not required to wear identification badges. In such a case, the visitor can simply remove the visitor badge and blend in with the regular occupants). Such a system not only facilitates visitor handling but also records visitor traffic. It also could be used to track the attendance of vendors and contractors. Some systems even allow visitors to self-register by using a scanned identification document, such as a driver's license.

After-Hours Access Register or Log. Whichever access control procedures are used, many office buildings maintain an *after-hours access register* or *log* to record after-hours access activity. This log includes details such as the person's name (printed for legibility) and signature, the name of the company the person represents or the tenant he or she is visiting, the date, and time in and out. In case of an after-hours building emergency, the log can be used to help ascertain who is in the building. However, the register or log does not provide a record of *all* persons in the building after hours, because some persons will have accessed the building during normal business hours before the access control log was in use. To determine exactly which tenants are in the building after hours, it would be necessary to telephone or to personally visit every tenant. Such a procedure, particularly in large office buildings, is not considered practical.

Right to Pass Signs or Plates. Signs or sidewalk plates, generally located outside the building, may state the following:

"RIGHT TO PASS BY PERMISSION, AND SUBJECT TO CONTROL, OF OWNERS" or "PERMISSION TO PASS REVOCABLE AT ANY TIME."

If a person who does not have a legitimate reason for being in the building is discovered, then the owner, manager, or agent acting on behalf of the building may revoke that person's right to remain. After being told to depart the premises, those who refuse to leave may be subject to arrest by law enforcement. Also, anyone reentering a building after having been warned that he or she is not authorized to enter may be treated as a trespasser.

Tenant Access Controls

Tenant access control involves *rented* or *assigned occupancies*. These are leased or owner-occupied spaces on various floors that are open to the public during normal building hours or restricted to identified and authorized persons. The access control measures for tenant areas vary from tenant to tenant, depending on their type of business activity, the design of the tenant space, and the individual tenant's management policy.

In some cases, visitors entering tenant space may simply enter at will and, in some instances, proceed directly to any area in the tenant space. However, in today's security-conscious world, many tenants require visitors to be greeted by someone and asked to submit to some form of verification procedure before being permitted to enter the tenant space.

Normal Business Hours

During normal business hours, most tenants in office buildings practice some form of access control. For larger tenants, often a receptionist is present at the main point of entry to act as the first line of defense.

Tenant space design varies from tenant to tenant; however, if possible, it is helpful to channel incoming persons through one area and keep all other access points properly secured. Some tenants establish a staffed reception area that is separated by physical barriers from the interior tenant space. Once a person has been cleared for admittance, the receptionist can allow entry.

Large companies that occupy several full floors served by one elevator bank can establish access control to their elevator bank at the street level. If there is no single elevator bank serving the tenant floors exclusively, the individual elevators can be programmed to each stop at one designated floor of that particular tenant. A reception area at this point can be used to control access to that tenant's other floors by way of an internal staircase or card-controlled access to the elevator. It is the responsibility of the receptionist (often in addition to answering telephones and handling other duties) to monitor both incoming and outgoing pedestrian traffic.

Only a receptionist who is properly trained to screen and handle incoming persons can enhance the security of the space. The receptionist must question people of all types to determine whether they are authorized to enter. One trick that has been used to gain access to office buildings has been for a person to pose as a photocopier or a telephone repairperson and, after gaining entry, proceed to steal purses, billfolds, petty cash, credit cards, laptop and notebook computers, and other small valuable items left unattended in the tenant space. These criminals are aided by two common practices: businessmen often hang their suit coat or jacket, containing their billfold, on a clothes stand or behind their office door; businesswomen, similarly, sometimes drape their handbag on a chair or leave it under their desk. These items can then be easily stolen. Another trick has been for an intruder, having gained access to a tenant space, to memorize a name from a desk or a directory board. If challenged by an occupant, the intruder simply states the name to avoid detection:

"Oh, I'm looking for Mr. Searcy!"

Unfortunately, on hearing such a reply, many an unknowing occupant has escorted the person to Mr. Searcy's desk and left the person there to continue with the deception. Such criminal behavior can occur more easily on open floors, where elevator lobbies open into corridors that, in turn, open without any form of barrier into the main floor areas (Figure 36-1).

Once it is established that a person is permitted to enter tenant space, the receptionist should arrange for entry in a manner that does not compromise security. The person may be issued a temporary "visitor" or "contractor" identification badge for the day and asked to fill in and sign the appropriate register. Then the receptionist may telephone the employee who is expecting the visitor and ask the person to come to the reception area to escort the guest. Also, some large firms and government agencies provide a corporate mailroom with a separate entrance where all couriers or others who are dropping off or picking up merchandise from the tenant space can be directed. This eliminates the need to escort these individuals separately.

Unwanted Solicitors. Receptionists can play an important role in building security by reporting solicitors they encounter. Solicitors may come to buildings with items for sale secreted in a bag or a briefcase. If they can obtain entry through the building lobby, once

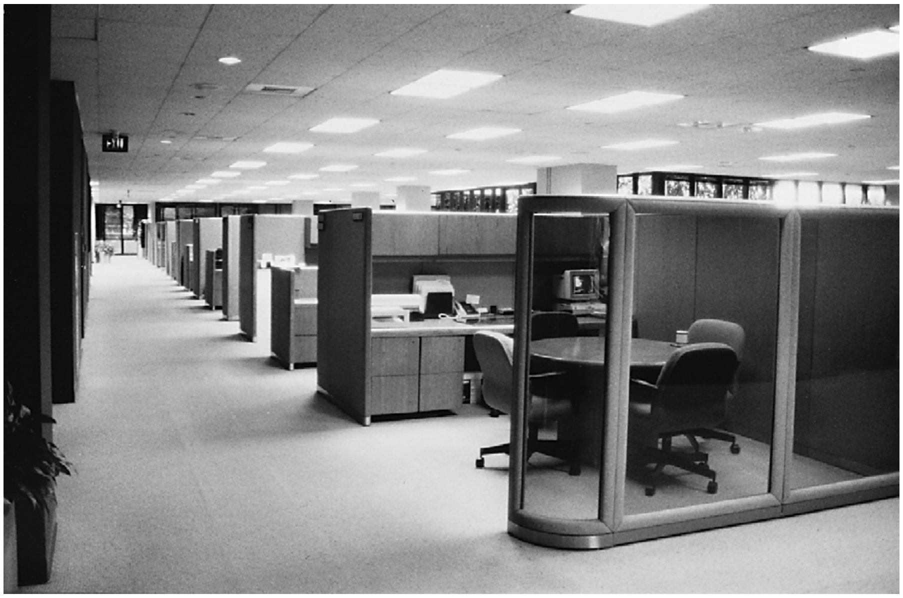


FIGURE 36-1 An example of an open floor viewed from near the passenger elevator lobby. *(Photograph by Roger Flores.)*

on a floor they will open up the container, take out their product, and proceed from floor to floor, tenant to tenant, selling their merchandise. Even though solicitors may be legitimate, their presence can be disruptive to tenant business; furthermore, criminals can pose as solicitors. The tenant should never buy anything the solicitor is selling. To do so provides an excuse for the solicitor to attempt to return to the building.

If a tenant receptionist detects an unwanted person such as a solicitor or someone who is behaving suspiciously, it is helpful to security staff if the receptionist can delay the person as long as possible until security assistance arrives. If possible, it is better to have a co-worker call for security personnel out of the solicitor's hearing range. Using a prearranged signal or code phrase — such as "Sarah, could you watch the telephones for me? I'm going to be busy with the flower seller for a few minutes" — may successfully delay the individual until security staff arrives. One way to detain a solicitor is to feign interest in the product and call other "interested" employees to look at the merchandise, preoccupying the solicitor. Other ways for the receptionist to detain suspicious persons would be to carry on a friendly conversation, offer an employment application, or use some other deception. Simply telling the solicitor that soliciting is not permitted generally is not enough. Having left that particular tenant, the individual will often go to other tenants.

For the protection of all tenants, it is best to have security personnel escort the solicitor out of the building. If it is not possible to delay the solicitor, it is helpful if the receptionist can at least notify security staff as soon as possible and supply a detailed description of the person involved, including physical characteristics and clothing details.

Tenant Security Systems. Some tenants have installed their own access control systems — electric locks, mechanical or electrical push-button combination locks, card-operated locks, biometric system-operated locks, or a combination of technologies — that control the operation of entry door(s) to tenant areas. Sometimes, CCTV systems, intercoms, and intrusion detection systems are used in conjunction with these devices. When considering a system, the local fire authority that has jurisdiction should be consulted to determine whether such an installation is permitted by local codes and standards; this is particularly important when the access control devices are to be installed on doors leading directly from elevator lobbies to the tenant space. These doors involve paths of egress during emergency evacuation and therefore require special locking arrangements permitted by the authority.

After Normal Business Hours

After normal business hours, in most office buildings, access control to all tenant areas is strict. Perimeter doors to the tenant space usually are locked when normal business is completed. Each tenant needs to establish a specific policy and procedure for access after this time. One possible solution is to furnish tenant entrance keys to all employees who require access. This approach, however, can lead to the same problems discussed earlier in the section Pedestrian Access to Buildings. Instead, some tenants issue keys only to a few select individuals. This alleviates some key control problems but creates the need for one of these persons to be present when special after-hours access is required. In some instances, building management has permitted some tenants to leave keys with security staff for special after-hours access. The tenant's employees must then return the keys to their representative on the next business day. Alternatively, if someone is present inside the tenant space, he or she may be telephoned by building security and notified of the request for entry or, according to a predetermined policy, the tenant may designate an on-call manager who handles such after-hours matters.

There is no clear-cut answer to the issue — factors such as the number of employees requiring after-hours access, the frequency of after-hours access, and tenant management's attitude toward its employees, as well as building management policies all need to be taken into consideration for a well-defined policy to be formulated. As noted previously, some tenants have installed their own access control systems to operate entry door(s) to tenant areas, possibly in conjunction with CCTV systems, intercoms, and intrusion detection systems. Other large companies who have around-the-clock operations provide security staff or receptionists to control after-hours access. Some maintain an after-hours access register or log similar to that required for the building itself. If the tenant is a restaurant that is open to the public after normal business hours and on weekends and holidays, there will be the need to provide easy access for the patrons and additional measures to ensure these persons cannot stray into other building areas.

Doors Locked. It is important that tenants never open their doors after normal business hours for anyone they do not know personally. For example, in an office building a temporary female employee working alone after hours one night opened the door to a man who claimed to be the window washer. The intruder raped the woman, then even had the nerve to say goodnight to the security officer posted in the lobby. Tenants should be educated that if someone belongs in their space, then the building or tenant management would have already provided them the means of obtaining access.

Escorts of Building Users

People in office buildings are escorted for a variety of reasons. It may be to accompany individuals for the purpose of protecting them or the property that they are carrying. It may also be to show a person where to go or to ensure that the individual does not remove property. In the high-rise setting, building users can be escorted to, from, and within the building and within tenant space.

Escorts to and from the Building. Escorts to and from a building usually occur after normal business hours. Security staff generally conducts these escorts. When tenants finish business, their employees, particularly females, may request building security to escort them to unsupervised areas of the property, such as parking garages. Building policy should dictate how, when, and where the escorts are to be conducted. For liability reasons, escorting people to off-site locations, particularly across streets, is not encouraged.

Escorts within the Building. Building policy may require that persons who need access to certain maintenance spaces and areas under construction or renovation are provided with an escort to accompany them whenever they are in these areas. Building engineering or security staff may be required to provide such escorts.

Some buildings have a list of local and state agencies whose inspectors are authorized to enter, but it is absolutely critical to verify such persons' identification and to make building management aware (if possible) of these persons' presence before they are granted entry. It is important to escort anyone claiming to be an inspector while he or she is in the facility. On occasion, professional burglars posing as local or state inspectors have been granted entry to buildings.

Also, janitorial staff may require escorts when they are removing trash material from building floors and transporting it to trash compactors and dumpsters. The purpose of the escort is to reduce the possibility of janitors transporting stolen items along with the trash from tenant floors and depositing them in places where they can be picked up later.

Escorts within Tenant Space. It is usual for visitors, such as salespersons, trades people, couriers, and delivery persons, to be escorted within tenant space. This will depend on the type of business the tenant conducts, tenant policy, and staff availability. For example, a tenant may require an employee to accompany such persons at all times while they are inside tenant space or just accompany them to particular areas and leave them unsupervised to carry out the tasks they have been authorized to perform.

Property Control

There are various property acceptance and removal systems that building managers and tenants can implement to provide some control over the property that on a daily basis is moved in and out of office buildings and tenant areas. The degree of control will vary from building to building and tenant to tenant, and it will depend largely on the policies established by building management and the tenants. The effectiveness of these policies will depend on how thoroughly they are communicated to building staff, tenants, and occupants; how strictly they are enforced; and the support afforded the program. It is sometimes difficult to implement strict property control measures in a multiple-tenant/multiple-use commercial office building, primarily because each tenant may expect a different degree of security. This discussion of property control does not include the means for protecting proprietary information. However, it is appropriate to mention that document destruction either on-site using a shredder or off-site by contract companies, can be an effective means of safeguarding critical information stored in documents that needs to be destroyed.

Objectives of a Property Control System. The objectives of a property control system are threefold:[23]

1. **To prevent stolen property or other unauthorized items from leaving**. Stolen property may include computers (personal, laptop, and notebook), personal data assistants, mobile telephones, fax machines, calculators, and general office equipment. An unauthorized item might be a sensitive or a classified document that is not to be removed from a certain area or from the building.
2. **To prevent dangerous items entering**. Explosives are the usual concern, but other items such as cameras or firearms might be prohibited. (As a result of September 11, 2001, metal detectors and X-ray systems, although not in common use in office buildings, were deployed in some landmark facilities as a screening measure for weapons and explosive material concealed on people and contained in packages and other containers.)
3. **To prevent unnecessary or disruptive delivery traffic**. By keeping out misdirected deliveries, unnecessary traffic is avoided. By routing deliveries through proper entrances, such as loading docks and freight/service elevators, disruptive traffic is avoided and, in some cases, the building and passenger elevators are protected against damage from hand trucks and bulky crates. By intercepting deliveries at these entrances to the building, it may be possible to detect intruders posing as delivery persons.

Property Removal Pass System. Unauthorized removal of property from office buildings can be controlled to a degree by requiring *property removal passes* for business and personal items taken through an egress point controlled by security staff. The time period when the property removal pass system is to be in effect is set by building management and then communicated to the tenants. (Some buildings only permit the checking of property removal after normal business hours.) Building management can supply property removal passes to key tenant representatives who then supervise their distribution to tenant employees and visitors on an as-needed basis. The passes may vary both in design and in the information recorded on them. However, small items can easily be concealed on a person or in a briefcase or a carrying bag. Also, a thief working in a building can circumvent a property control system by using commercial mail services to send stolen items out from the building. Unless electronic tracking of assets is provided, a thief can thereby bypass a building's property control system.

Required Information for a Property Pass

For the property pass to be of value, it should address at least the following areas of information:

- Name and signature of the person authorized to remove the property
- Name and room or suite number of the tenant or company from whom the property is being removed
- Printed name and signature of the tenant representative who has authorized the property removal
- Brief description of the property, including any model, serial, or asset tag numbers
- Date property will be removed (some passes do not require this information)
- Date and time of removal of the property
- Signature of the person (usually a member of the building security staff or a receptionist) collecting the pass and permitting removal of the property.

Property passes should be sequentially numbered and a record kept of which tenants received which numbered passes. They should also be in duplicate (following the removal of the property, the original is returned by the building security staff to the tenant representative and a copy is kept on file by the building security department).

A *sample property removal pass* for an office building is shown in Figure 36-2. After the authorized tenant representative has signed the form, any blank lines on the pass should be crossed out to prevent unauthorized entries.

Whenever building security staff reviews a property removal pass, they should thoroughly examine it to ensure that it is complete and contains all the necessary information. The identity of the person actually removing the property should be confirmed by means of a valid driver's license or other photo identification.

It is best if each tenant has already provided an authorization letter containing sample signatures of each representative authorized to sign a property removal pass. Building security staff can then compare the signature on the pass with the signature on the letter. If it matches, security will permit removal of the property. If it does not match, security personnel will keep the pass and may attempt to contact an authorized tenant representative or building management to resolve the matter. Such a system can be effective in controlling the removal of some business and personal property. However, as previously mentioned, many computer-related items are small enough to be carried out unobserved in a carrying case or pocket.

Permanent Property Pass

Some office buildings permit the use of a *permanent property pass*. This pass eliminates the need to continually issue property passes for personal or company property that is frequently carried in and out of the building. The permanent property pass is similar both in design and recorded information to a regular property pass, except that it can be used repeatedly for the period of time stipulated on the pass. The card is often laminated to prevent damage and affixed at all times to the item in question. Building security staff should keep a photocopy of each pass and a log that documents their use. Of course, if the pass is lost or the tenant cancels its usage, building security must be notified immediately.

Asset Tracking Systems. Small radio frequency identification (RFID) asset tags — some of which were embedded into desktop and laptop computers at the time of manufacture — can be assigned to an asset that is permitted to leave a building. Integrated with a building's access control system, asset tracking can be utilized to control the movement of computer equipment and other assets from the building.

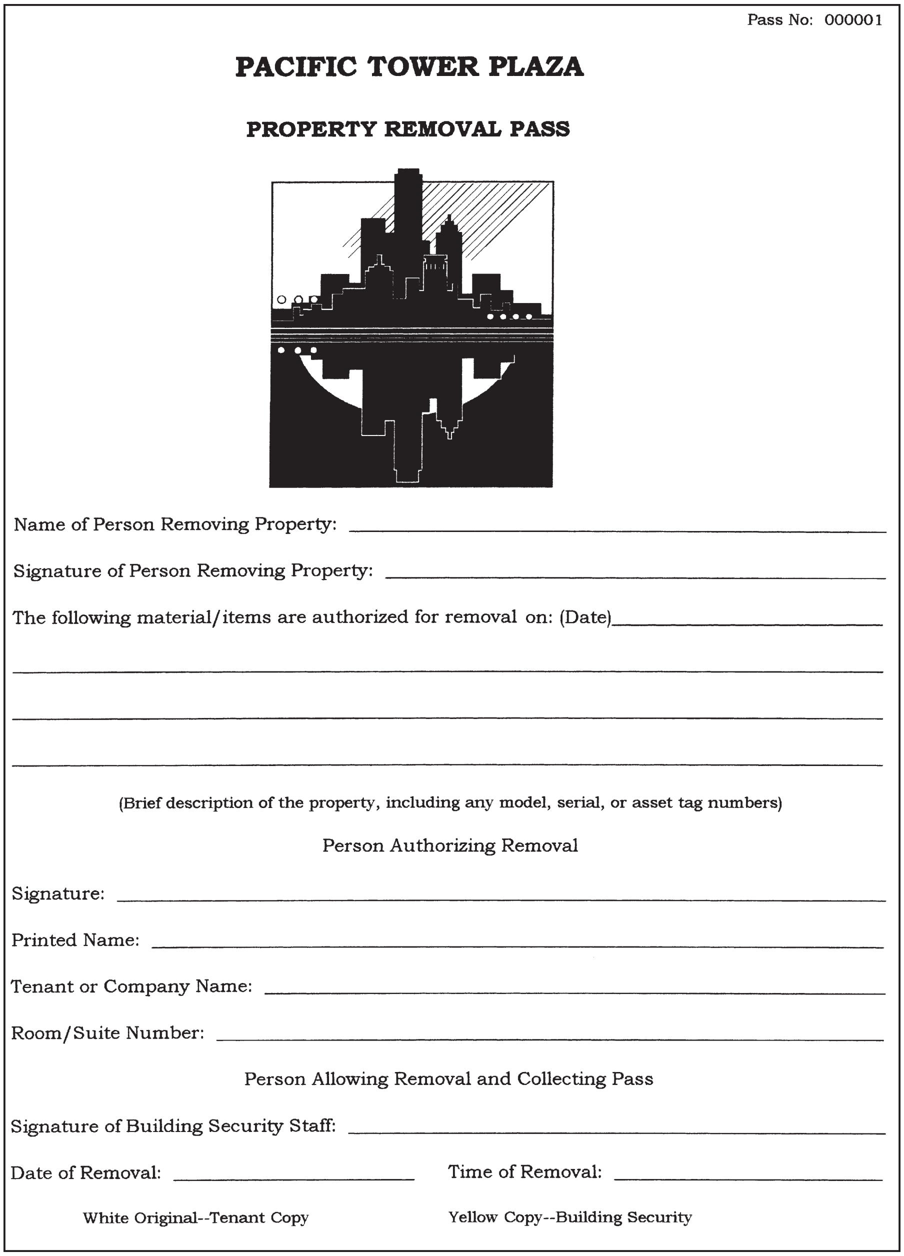
An asset tagging and tracking proximity system "allows free egress when authorized assets are removed, but prevents unauthorized removal of property. Without electronic tracking, assets can be removed by concealing them in a briefcase, package or gym bag."[24] This system can also be adapted to screen assets that are mailed out of a building through a central shipping area such as the loading dock.

Dangerous or Illicit Items. To prevent someone from entering the building on foot or in a vehicle with dangerous or illicit items is not as easy a task as it would seem. Items such as explosives, illegal drugs, and chemical and biological weapons might easily be secreted on a person or in a vehicle and brought into a building.

Measures to Screen for People-Delivered Explosive Devices

The following is a list of various measures that can be used to screen for persons possibly bringing explosive devices into a building:

- Search persons and items such as suitcases, briefcases, handbags, gym bags, backpacks, packages, and other containers. This practice is not common in most commercial office buildings.
- Use metal detectors and X-ray machines, explosives trace detectors, or explosive-detection trained (bomb-sniffing) dogs to screen for weapons and explosive devices concealed on people or in items



Pass No: 000001

PACIFIC TOWER PLAZA

PROPERTY REMOVAL PASS

Name of Person Removing Property: ____________________

Signature of Person Removing Property: ____________________

The following material/items are authorized for removal on: (Date)____________________

____

____

____

(Brief description of the property, including any model, serial, or asset tag numbers)

Person Authorizing Removal

Signature: ____________________

Printed Name: ____________________

Tenant or Company Name: ____________________

Room/Suite Number: ____________________

Person Allowing Removal and Collecting Pass

Signature of Building Security Staff: ____________________

Date of Removal: ____________________ Time of Removal: ____________________

White Original--Tenant Copy Yellow Copy--Building Security

FIGURE 36-2 Sample property removal pass.

they carry. Due to the perceived high-risk, some landmark buildings are deploying such measures.

- Keep doors or access ways to certain areas — mechanical rooms, mailrooms, computer rooms, data centers, and elevator machine rooms — locked at all times.
- Install intrusion detection devices at entrances to high-risk areas, and use CCTV in areas identified as likely places where a bomb may be placed. This, coupled with posting signs indicating that such measures are in place, is a good deterrent.
- Building personnel should be alert for people who act in a suspicious manner, as well as objects, items, or parcels that look out of place or suspicious.
- Security personnel should patrol potential hiding places (e.g., stairwells, restrooms, and vacant office space).
- Good housekeeping should be practiced for trash (rubbish) storage, trash compacting, and dumpster areas. (Likewise, a sometimes overlooked possibility is that when a fully loaded dumpster is replaced, one loaded with explosive material could be delivered. Dumpsters should be checked upon delivery to ensure they are empty.)
- Mailboxes at buildings can be used to deposit an explosive device for later detonation. Consideration should be given to using blast-resistant mailboxes or to removing them altogether.

Measures to Screen for Vehicle-Delivered Explosive Devices

Measures to reduce the risk of explosive devices in vehicles include the following:

- Restrict or eliminate parking of vehicles adjacent to a building, and eliminate public parking in underbuilding parking garages.
- Check passenger vehicles, particularly those entering underbuilding parking garages, for bombs as they enter. For high-risk facilities, these inspections might include the use of security or parking personnel inspecting vehicles (including their trunks and boots) or using a small hand-held mirror or a CCTV camera attached to a 3 × 4-foot (0.91 by 1.21 m) long metal pole to inspect under vehicles, undervehicle scanning systems, and the use of explosive trace detectors or explosive-detecting (bomb-sniffing) dogs.
- Require vehicles, particularly vans and trucks, to undergo on-street inspections before being permitted to enter loading dock/shipping and receiving areas. For high-risk facilities, these inspections might include performing X-rays of entire vehicles, the use of undervehicle scanning systems, and the use of explosive trace detectors or explosives-detection trained (bomb-sniffing) dogs.

Couriers and Delivery Persons. In many facilities, couriers and delivery persons, once cleared to enter, can freely move about a building to deliver and pick up letters, packages, and other items from tenants. However, there is an alternative for owners and managers who want to prevent unnecessary, disruptive, or possibly undesirable delivery traffic in their facilities. Some buildings have instituted special programs whereby outside couriers, on arrival at a building, are directed to a separate entrance, such as the loading dock or a central mailroom. At that location, building couriers employed by a contract courier or a security company assigned to the building sign for the items and deliver them within the building by way of the freight/service elevators. When items are to leave the building, these same couriers pick up the articles from the tenants, bring them to the central location, and then outside courier companies sign for them before taking them from the facility. As a rule, major courier services that regularly do multiple deliveries in a building are permitted to perform their own pickups and deliveries. Special deliveries or pickups can be facilitated by providing temporary badges for outside couriers to enter or by providing an escort for these couriers while they are in the building.

These programs have been very successful. When dedicated building courier or security staff performs multiple deliveries and pickups from tenants, the overall number of couriers roaming throughout a building decreases: a valuable security advance when a million square foot office building may have 300 or more individual deliveries per normal business day. In addition, the number of couriers using elevators is reduced. Also, it can enhance security by providing an added presence in the building (particularly if security staff are used), and because these building couriers should have already been "security vetted" (i.e., a background check of these individuals has been conducted), there is less chance of possible theft or vandalism than when using outside courier services. Delivery to secured or normally "locked-off" floors is also easier because dedicated building couriers can more readily be entrusted with the access codes or cards that allow them to enter such restricted areas.

Like any well-run operation, such programs need to be meticulously documented to provide an audit trail to track deliveries and pickups and ensure that these tasks are being done in a timely manner. If there is a question about the time property was picked up or delivered or about the individual who signed for it, accurate records should be immediately available for review. Some individual tenants, particularly larger ones that occupy full floors and multiple floors, have addressed the issue of outside couriers roaming within their space by establishing a separate mailroom from which only tenant messengers perform all deliveries within the tenant area.

Package Acceptance Policy. During normal business hours, when tenants are usually open for business, they generally accept their own packages. For those delivered after hours, their acceptance or rejection largely depends on the policy established by the building owner or manager. For security and safety reasons, most commercial office buildings do not permit after-hours acceptance of packages by security staff. The building does not want to accept the responsibility and potential liability of accepting packages (including certain legal documents) the tenant may refuse; also, these packages may contain dangerous or illicit items. Some buildings do permit the acceptance of after-hours packages on certain occasions and under special circumstances. This will usually require a written request by the tenant and an explicit understanding that the building and its agents are absolved from any liability resulting from accepting the package on behalf of the tenant.

Lost and Found Property. Handling lost and found property is an often-neglected but critical part of an effective security program. Most people can recall the anguish they felt on discovering that a valuable personal possession or business item was missing. Likewise, one may remember the exhilaration at being contacted and informed that the missing property had been found and was available for pickup.

If property is lost in a building and is subsequently found and handed to building security staff, the item(s) should be kept in a secure place (such as a locked cabinet or an access-controlled room) and, if possible, expeditiously returned to its rightful owner. Such action can considerably enhance the trust and confidence that building occupants and visitors will have in the building security operation. Just the opposite will be true if a tenant learns that the found item was handed to building security staff and was then lost or went missing.

Lost and Found Property Log

Building security staff should maintain a list of lost and found items in a *lost and found property log*. The log should contain details such as the following:

- A brief description of the property, including any serial or asset tag numbers
- The date, time, and place the property was lost or found
- The identity of, and means to contact, the person who lost or found the property
- If the property is claimed, the identity of, and means to contact, the claimant and the signature of the person who received the property
- The name(s) of the person(s) who took the report of the lost property, logged in the found item(s), or handled the return of the property to its rightful owner

Handing Over to Local Authorities

If the lost property is particularly valuable or sensitive, it may be necessary for the local law enforcement agency to be contacted; if the property is subsequently handed over to them, this fact, including the identity of the receiving law enforcement officer, should be noted. A receipt for the property should be obtained. Local and state laws often determine the handling of lost property.

Some jurisdictions allow found property, when its owner is unknown and its value is below a certain amount, to be distributed to local charitable organizations. Others, after a certain waiting period, auction the property or allow the finder to assume ownership of it.

Trash Removal Control. There are a number of controls that can be placed on trash removal from tenant space and from a building. The design and implementation of these controls largely depend on the specific cleaning operations in effect at the building. Some operations “gang clean” by using a team (including dusters, cleaners, waxers, polishers, and trash removers) to clean tenant spaces and restrooms on a series of floors. Others assign specific janitorial staff to perform all functions on particular floors. From a security standpoint, the latter is preferable because regular staff members are more likely to detect unauthorized persons who do not belong in a particular tenant space, and because investigations involving janitors are easier when the same janitors regularly work in a particular tenant space.

Sensitive Information

Depending on the sensitivity of the business conducted, tenants may shred certain proprietary documents themselves, or they may employ contract-shredding agencies that will come to the building on a scheduled basis to remove and destroy documents. These documents may include sensitive business data, client lists, and billing information, those that are confidential within a company, and any proprietary information that would be useful to competitors. Depending on the sensitivity of these data, they may be passed through a standard shredder or through a crosscut shredder.

Importance of Supervision

Routine removal of trash from a tenant floor should be carried out under constant supervision by janitorial supervisors or building security staff. No interruption should take place in supervision during the janitors’ passage from the tenant floor to a service or freight elevator or to designated receptacles such as dumpsters, compactors, or holding areas, usually located at the building loading dock. Such supervision will deter janitorial staff from secreting stolen articles in trash bags and then dropping the articles in locations within the building where they or an accomplice can later retrieve them.

To make it easier to scrutinize trash, the bags should be made of transparent plastic. If, because of staffing limitations, direct supervision of trash removal is not possible, then CCTV cameras in the dock areas are recommended to deter the removal of items from trash bags before they are placed in dumpsters, compactors, or holding areas, or for later retrieval from the receptacles.

Special Trash Holding Areas

Trash holding areas can be found in office buildings, particularly where refuse from financial institutions is being handled. To avoid accidentally discarding important documents such as negotiable instruments (checks, bank drafts, savings bonds, securities, etc.), the trash from financial businesses often is separated and held in a secured area for a length of time as determined by the financial institution concerned. The holding time permits losses to surface before trash is removed for destruction, thereby facilitating possible retrieval of the item in question.

Janitorial Staff Screening. In many buildings, janitorial staff may be required to enter and leave the building through an employee entrance and be subject to certain property screening procedures. The object of the screening procedure is to observe any prohibited items being brought into the building and to detect any stolen property being removed from the building. As part of pre-employment or pre-assignment agreements, janitors may be asked to submit to a visual inspection of any items they are carrying to and from work — lunch pails, bags, backpacks, packages, and other containers. The frequency of the inspections can be established as part of the agreement: inspections may be conducted every time the employee enters or leaves the building, at random, or only with cause.

Janitorial supervisors or building security staff usually conduct such inspections. They are visual only, and employees are requested to open appropriate items themselves. Under no circumstances does the inspecting person touch the items being inspected or attempt to inspect any part of the employee's person or clothing. All persons have a legal right and expectation of privacy, so items such as purses will be subject to inspection only under special circumstances, the nature of which should be established in writing beforehand. Some operations require janitorial staff to wear special clothing or smocks in which it is difficult to conceal items.

Importance of Controlled Ingress and Egress. The success or failure of any property control system depends largely on whether there are "controlled" exits or entries to the facility for use by building occupants and visitors. For example, if building users need to pass through one particular point to enter or leave the building, and if this point sometimes is not supervised, then the property control system can be circumvented. Similarly, if there are other unsupervised exits or entry points, persons can defeat the property control system by using these areas when they want to bring in or take out property.

Some high-rise buildings with underbuilding parking garages have passenger elevators that allow people to travel directly up from the garage to the tower and similarly for people to travel directly down from the tower to the parking garage. Such an arrangement affords no control over ingress and egress of people and property.

To address this problem, there are several possible solutions:

- **Whenever the elevators are operating, provide security staff in the parking garage elevator lobbies**. This will help control the movement of people and property, but it is an ongoing security expenditure.
- **Install optical turnstiles in the parking garage elevator lobbies.** This will control the movement of people but will not control property (and the turnstiles will require some supervision by security staff).
- **Install full-height security turnstiles equipped with card readers in the parking garage elevator lobbies**. This will control the movement of people but will only control large property items.
- **Install card readers in the elevators**. This will help control the movement of people (tailgating or piggybacking of passengers will be possible) but will not control property.
- **Install CCTV cameras in the elevator cars or in the parking garage elevator lobbies**. If the cameras are constantly monitored or the images constantly recorded, the unauthorized movement of property might be observed either at the time it occurs or at a later stage.
- **If possible, reprogram the elevators so that some exclusively service the parking garage and the building main lobby**. Passengers traveling up from the parking garage will need to cross to other elevators to proceed to the tower floors. Similarly, passengers traveling down from the tower floors will need to cross over to the garage shuttle elevators to proceed to the parking garage. (Due to the limited numbers of elevators in some buildings and the pedestrian traffic load, such a measure may not be practical due to congestion and extended delays.) Even with this arrangement, to effectively control most property, the main lobby would need to be staffed by trained security personnel. If such staffing is not possible because of budgetary constraints, card readers may be provided in the elevators and CCTV cameras placed inside all elevators or at the parking garage elevator lobbies. By placing the elevators on card access, tenants will be required to use their cards to access floors, thereby providing some degree of access control. If the cameras are constantly monitored or the images constantly recorded, the unauthorized movement of property might be observed either at the time it occurs or at a later stage.

Key and Electronic Access Card Control

In office buildings, keys and electronic access cards to the facility are under the control of building management, engineering, and usually security personnel. Building management personnel obviously need to have access to all areas of the facility they manage. Building engineers, because of the nature of their work, also need access to virtually all areas, including tenant spaces. Depending on how the building is managed, security staff also will need access to most areas.

Key Control. The decision as to whether master keys are issued to building security staff will vary from building to building. If they are not issued master keys, they will often be issued a ring of keys permitting them to enter various parts of the building. Some facilities keep tenant office keys out of the routine possession of security staff but provide a controlled, documented means for these keys to be obtained, when necessary. After the situation has been resolved, the keys are again placed under supervision, perhaps in a locked cabinet or a key cabinet secured with a key, a lock code, an access card, or a consecutively numbered seal.

Keys issued to the security staff should never be permitted to leave the facility. They should be passed from shift to shift and a receipt should be recorded each time they change hands. All security personnel should understand the importance of not permitting keys to be compromised.

Key Points to Consider

Keys (and access cards) should be issued only to those persons who can be entrusted with them and who have an *absolute* need for them. The status a key holder may feel by possessing certain keys should not enter into the decision-making process. The following points are important to consider:

- Tenants and residents should be issued keys that pertain to their particular area only.
- Tenants and residents should never be issued building entrance keys. (If issuing entrance keys is unavoidable, the locks should be changed periodically or when a key has been lost or taken, and new keys should be issued to the tenants authorized to have them.)
- Tenants and residents should not be allowed to duplicate keys. (Keys should be marked "Do Not Duplicate" as a deterrent to duplication. Also, keys issued to tenants may be distinctively marked to help identify unauthorized keys they may have had cut themselves.)
- When an employee ceases to work for a tenant, all the employee's keys should be returned to the tenant representative. Depending on the situation, locks may need to be changed.
- When a tenant or a resident moves out, all tenant or resident entry door locks should be changed.
- Janitorial staff should be issued keys only for the time they require them and for the particular areas to which they require access. Depending on the size of the janitorial staff, designated supervisors within the janitorial operation may be issued master keys that, for instance, provide access to all tenant spaces on an individual floor. In this way, the general cleaning staff does not need to be issued keys. In some buildings, no janitorial staff is issued keys, and security staff must unlock the appropriate doors and relock them after the work is completed. Procedures will vary from building to building depending on size, complexity, and the manner in which cleaning is conducted and trash is removed.
- Elevator, escalator, dumbwaiter, chute (rubbish, mail, laundry, and linen), and moving walk technicians may be permitted to carry keys that provide access to their equipment, or the building may retain possession and issue them only as needed.

In some buildings, telecommunications technicians, gas, water, and power utility workers are permitted to attach their own locking devices to areas containing their equipment. This practice is convenient because the building staff is not required to open these areas, but it compromises security because control of keys and the areas themselves has been lost. These areas could be used to store unauthorized or stolen items, and general housekeeping may become a problem. If this practice is permitted, no one should be allowed to place a lock on a door without building security or other building departments (such as engineering) having a key. In an emergency, keys must be available for access. A possible alternative is for contractors to store their equipment, including tools, in heavily reinforced, large steel boxes, chests, and cabinets that can be secured using high-security padlocks, which are protected from attack with cutting tools.

In the event of a lost or missing key, the circumstances surrounding the incident should be investigated and documented. If the key has been compromised, consideration should be given to changing the affected lock(s) or moving it to a less sensitive area of the building; in the case of a compromised master key, because the whole system is compromised, rekeying the entire building should be considered. "If rekeying becomes necessary, it can be accomplished most economically by installing new locking devices in the most critical points of the locking system and moving the locks removed from these points to less sensitive areas. Of course, it will be necessary to eventually replace all the locks in the system, but by using the method just described, the cost can be spread out over several budgeting periods."[25] Whether to immediately rekey the building or delay in this suggested manner is a risk-based decision that should only be undertaken by the building owner or manager. If delaying the rekeying can potentially affect the life safety of people or seriously impact other vital assets, then despite the costs involved, it should not be delayed.

Electronic access cards should be issued only to those persons who can be entrusted with them and who have an *absolute* need for them. Access cards issued to building staff, including security staff, should never be permitted to leave the facility. They should be passed from shift to shift and a receipt should be recorded each time they change hands. All personnel should understand the importance of not permitting access cards to be compromised. Also, if a card is lost or missing, as soon as possible after its reported loss, it should be deleted from the system and the circumstances surrounding the event investigated and documented.

Mobile Patrols

Mobile patrols may be conducted in office buildings for a variety of security and fire life safety purposes. "Guards [security officers] are typically highly visible thus offering something of a deterrent effect and at the same time imparting a sense of security to the building's tenants and visitors."[26] Patrolling increases this visibility. Patrols can also be used to note and quickly address anything significant or unusual affecting security or fire life safety. After conducting a risk assessment, the purpose, frequency, and routing of patrols can be determined by hotel management and the security department (and, if special circumstances warrant, with the cooperation of local authorities) and then carried out and thoroughly documented.

When and Where? Patrols by security staff in office buildings may occur as follows:

- For approximately the first hour after opening the building on a regular business day, when there are usually not many occupants in the building, to provide a security presence *throughout common areas and tenant floors*.

- *After the building is closed at the end of the business day, on tenant floors*, to check for doors left unlocked or not completely closed, signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong, and so on.
- *Some buildings require such patrols continuously throughout all common and maintenance areas (including stairwells outside normal business hours)*. The purpose is to report obstructions (particularly those blocking emergency egress routes), fire hazards, missing equipment (such as portable fire extinguishers), water or gas leaks, wet floors, holes, defects in floor coverings, tiles missing, unsecured areas, malfunctioning lighting equipment, signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong, and so on.
- *Continuously in parking garages and lots* to deter theft of vehicles and property within them; note parking violations (including vehicles improperly parked, parked in a NO PARKING zone or space, parked in a RESERVED zone or space, or parked in a DISABLED/PHYSICALLY IMPAIRED designated space), and issue warnings or citations, or institute vehicle towing actions; observe vehicle lights or engines left on, leaks from vehicles, or other unusual conditions of parked vehicles; report fire hazards, water or gas leaks, malfunctioning lighting equipment, broken vehicle windows and other signs of forced entry, unauthorized and suspicious persons, and others (including building staff) found in areas in which they would not normally belong; and provide for the general safety of tenants and visitors. (Motor vehicles, electric carts, bicycles, tricycles, and personal transporters may be used for patrolling large parking areas with long travel distances.)
- On building floors and in parking garages, key patrol stations are often installed *at each stairwell* so that the patrolling officer must traverse the floor in order to complete the tour.
- Depending on a building's usage, patrols may also be conducted in areas such as *retail arcades, public parks and gardens, and other areas, with times varying according to their operating hours*.
- *In some buildings, patrols within tenant spaces* to report security and safety hazards, including unsecured laptops and confidential information. Keep in mind, entering a tenant office may place the patrol officer in a "difficult and sensitive" situation, particularly after normal business hours. If it is necessary for a security officer to enter a tenant area after hours, another officer should accompany him or her. These officers should knock on the door before opening it and call out loudly to identify themselves and their intentions. Such actions can help avoid embarrassing and awkward situations and protect staff from unfair accusations. If entering tenant space is only permitted under special situations, it may be wise to also be accompanied by a building engineer or other building staff member. Intrusions into tenant space should always be thoroughly documented.
- *To perform a fire watch when a building has exceptional hazards or the fire protection system is impaired*. A fire watch is "the assignment of a person or persons to an area for the express purpose of notifying the fire department or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety dangers."[27]

Patrolling Tips

- Patrols can be conducted on foot or using a motor vehicle, an electric cart, a bicycle, a tricycle, or a personal transporter.
- There should be reliable communication between the patrolling officer and the security department or the supervisor.
- Whenever possible, routine patrols should be conducted in a random, unpredictable manner to avoid a fixed pattern or routine that someone planning to commit a crime can observe. Sometimes, an officer occasionally "doubling back," or retracing steps to a previous location, can be an effective tactic; anyone observing the patrolling officer's movements would usually not expect the officer to return quickly to an area just visited.
- "Alertness, interest and thoroughness must be displayed. A suspicious mind must be cultivated and anything that appears other than normal must be looked into."[28]
- Using a flashlight or a torch in areas where lighting is poor or nonexistent is extremely useful.
- "A simple but effective patrol plan should be established in each area. Its efficiency should be regularly checked by means of patrol management devices, radio or telephone checks at regular intervals, etc. Failure to report, or deviation from described assignments, should immediately be investigated."[29] Patrol management devices "provide the security manager with a consistent record of rounds and occurrences at a facility without the need for human supervision to ensure that rounds are completed as assigned."[30] If an electronic patrol management device is not used, a notebook is useful for recording observations. (The patrolling officer can carry the notebook, or it can be located at designated patrol stations so the officer can record when visiting a particular area.)

Tenant Security Education

There are many ways to educate building users and tenants about the building's security program. All building users, particularly tenants and their visitors, should be made aware of the program and how various policies and procedures impact them. If people are aware of the logic behind security regulations, they usually will be more willing to comply with them. This communication can be achieved in the following ways:

1. Explain the regulations on an informal, as-needed basis. For example, building security staff may explain the purpose of an after-hours access register to a tenant when asking him to sign it, or staff may inform a visitor leaving the building that she must have a property removal pass signed by the tenant she just visited before the computer she is carrying can be permitted to leave the building.
2. Use posted signs; written policies and procedures published in the Tenant Manual and on the building's Web site; pamphlets, leaflets, flyers, newsletters, e-mails, and video training materials supplied by building management to the tenant or by tenant management to its employees. Sometimes, information is displayed on in-car elevator video screens. Such elevator bulletins may, for example, provide information that reminds occupants that in the event the elevator stops running, they should immediately use the elevator emergency communication device to request assistance, or the bulletins may be used to post other appropriate emergency notifications.
3. Conduct security and safety orientation lectures, classes, briefings, workshops, and seminars. These events can be an effective medium not only for communicating to tenants what is required of them in the building security program, but also as an opportunity to educate employees about basic security and safety measures they can adopt at home. (Such measures could include being aware of their surroundings; elevator safety; securing vehicle doors and windows; not leaving valuable items in view in parked vehicles; securing desks, filing cabinets, laptop computers, computer storage devices, and personal property; and observing a "clean tabletop" policy.) The length of such events will vary, but 45 minutes to an hour is probably the maximum that busy tenants will permit. As with all effective teaching, the use of audio-visual aids — films, videotapes, DVDs, and slides — can help gain the participants' attention and assist in effectively communicating the required message. The frequency of classes, meetings, conferences, seminars, and workshops will vary from building to building; they may be regularly scheduled or conducted when a specific need arises. Security training can be incorporated effectively into occupants' fire life safety training classes. More will be said about the training of occupants, floor wardens, and building emergency staff in the next section.

Tenants are an important part of any building security program. They should be educated to know that they are the eyes and ears of the building. If they see a suspicious person, particularly someone within their own tenant space, a simple "May I help you?" type of approach will reveal much about the person. Specific questions can determine if the person is an employee, a visitor (if so, who is he or she visiting?), or is delivering or picking up items (if so, where? at whose request?), and so on. Although the tenants are not expected to be trained security professionals, they are expected to be active participants in the building security program by being aware of their surroundings and promptly reporting potential security problems to tenant management, building management, and building security staff.

EMERGENCY PLANNING

For a building owner or manager to effectively manage an incident that constitutes an emergency in an office building, it is critical to plan ahead. Before proceeding, it is appropriate to review several key concepts.

Key Concepts

An *incident* is an "event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization's operations, services, or functions — which, if not managed, can escalate into an emergency, crisis, or disaster."[31]

A *disruption* is "an event that interrupts normal business, functions, operations, or processes whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a [power] blackout, terror attack, technology failure, or earthquake)."[32]

An *emergency* is "an event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response."[33] During an emergency there may be chaotic conditions, particularly if there is a disruption in normal communications.

A *crisis* is "an unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment."[34]

Emergency management (also sometimes known as crisis management) is defined as "the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness [and] response."

A *plan* is defined as "a scheme or method of acting or proceeding developed in advance."[35]

Combining the terms *emergency management* and *a plan* can lead to a definition of an *emergency* *management plan* as "a scheme or method of acting or proceeding developed in advance for the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness and response."[36]

"The objective of an [emergency management plan] should be to allow those responsible for the [facility] during an emergency to focus on the solution of major problems, not to attempt immediately to bring order out of chaos. If all predictable and routine items are considered in the plan, those responsible for actions during an emergency will be able to deal with the unpredictable or unusual situations that will surely develop."[37]

According to Groner,

> *The chaotic and dynamic nature of building emergencies requires an exceedingly rapid assessment of the situation. The timeframe is measured in seconds and minutes, not hours and days. The rapid onset of many events means that the process should be well underway before emergency responders arrive at the building.*
>
> *Human factors professionals have been actively researching this problem under the generally accepted term of "situation awareness." Endsley (1988) has provided a well-accepted definition: "The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."*[38] *As noted in the definition, it is insufficient to understand the momentary status of the situation; projecting its development is of great importance in choosing a strategy to safeguard building occupants.*

The purpose of an emergency management plan is to help building emergency staff in their efforts to achieve situation awareness and make sound decisions to provide for the safety of building occupants during emergencies, such as fire.

The value of emergency planning lies not only in the emergency management plan itself but also in the development process leading up to it and the education of building emergency staff that should occur in the process.

How to Develop a Building Emergency Management Plan

The building emergency management plan is a suggested format for developing an emergency management plan for an office building. It includes actions intended to reduce the threat to the life safety of building occupants from emergencies, both fire and non-fire-related, that are likely to occur in a specific building, or in close proximity to it, until the arrival of emergency responders.

It is important that as many as possible of those who will be involved in the execution of the emergency management plan participate in the planning process. This includes the emergency staff of the building, public officials (such as those from the local fire and law enforcement agencies), and possibly building management staff from neighboring buildings (with the view to developing mutual aid agreements). Public officials may require a particular format for the plan itself.

SUMMARY

- From the time a vehicle enters an office building parking structure and pedestrians proceed to the building, travel in the tower elevators, and enter an individual tenant space, there is a need for access control measures that sift out unwanted persons and intruders and yet constitute a minimum of inconvenience to legitimate building users.
- In multiple-tenant commercial office buildings, the three lines of defense — the main lobby, the elevators and lobbies on each floor, and the entrances to tenant space — provide points at which access can be controlled.
- Personal and business property that is moved in and out of an office building and tenant areas must be controlled. To establish a successful property removal control system, there must be supervised egress points through which all property and trash should pass. Tenants are a vital part of security and must be educated in security awareness.
- The purpose of establishing, implementing, and maintaining a building emergency management plan is to provide for the life safety of all building occupants.

Key Terms

area of refuge A designated area of safety for occupants inside or outside of a building. Also known as a *safe refuge area* and an *area of rescue assistance* inside a building.

area of rescue assistance "An area that has direct access to an exit, where people who are unable to use stairs may remain temporarily in safety to await further instructions or assistance during emergency evacuation."[39] Also known as an *area of refuge* or a *safe refuge area* inside a building.

business continuity planning "An interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption."[40]

courier A person or a company that delivers or picks up items such as documents, parcels, packages, or containers.

credential Something that entitles a person to certain rights or privileges.

crisis "An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment."[41]

crisis management See emergency management.

defend-in-place A strategy that "recognizes that at times it is safer for occupants to remain in place within protected zones of a building than to evacuate the building."[42] Sometimes known as *shelter-in-place*.

delayed evacuation This strategy "takes advantage of temporary holding places, typically known as areas of refuge or areas of rescue assistance, where occupants can remain in relative safety, albeit near the fire area, for a period before evacuating the building, either by themselves or with assistance from emergency responders or others."[43]

disability "A physical or mental impairment that substantially limits one or more of the major life activities of such individual."[44] "People with physical disabilities rely on a variety of artificial means for mobility. Such devices range from canes and walkers to motorized wheelchairs."[45]

disabled assistance monitor A person who locates disabled/physically impaired and nonambulatory persons and assists them to the nearest "area of rescue assistance." See *area of rescue assistance*.

disruption "An event that interrupts normal business, functions, operations, or processes whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a [power] blackout, terror attack, technology failure, or earthquake)."[46]

drill "An exercise involving a credible simulated emergency that requires personnel to perform emergency response operations for the purpose of evaluating the effectiveness of the training and education programs and the competence of personnel in performing required response duties and functions."[47] See also *fire drill*.

dumpster "A large steel waste receptacle designed to be emptied into garbage trucks. The term is a genericized trademark of the Dumpster brand. The term is also common in Australia, although Dumpster is not an established brand there. In British and Australian English, the terms wheelie bin and skip are more commonly used (although they are not perfect synonyms). In some other countries the more descriptive term frontloader container is often used, either in one or two words. In India it is called a *garbage bin*."[48]

elevator monitor Person who directs all passengers who arrive at his or her floor to proceed to the nearest safe stairwell and prevents any occupants from using the elevators for evacuation during a fire emergency.

emergency An "event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a significant and coordinated response."[49]

emergency action plan (EAP) "Designated actions that employers, employees, and other building occupants should take to ensure they are safe from fire and other emergencies."[50] See also *emergency management plan*.

emergency management "The organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness [and] response."[51] Also known as **crisis management**.

emergency management plan "A scheme or method of acting or proceeding developed in advance for the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness and response."[52] Sometimes referred to as a *fire safety plan* or an *emergency action plan*.

emergency operations center (EOC) "The physical location where an organization comes together during an emergency to coordinate response and recovery actions and resources. These centers may alternatively be called command centers, situation rooms, war rooms, crisis management centers, or other similar terms. Regardless of the term, this is where the coordination of information and resources takes place."[53]

fire drill A fire drill is an exercise for a simulated fire emergency. See *drill*.

fire safety director This person establishes, implements, and maintains the building emergency management plan. Sometimes known as the *life safety director, life safety manager, building evacuation controller, or emergency coordinator*.

fire safety plan See *emergency management plan*.

fire warden See *floor warden*.

fire watch Patrols at appropriate intervals determined by the fire department may be required when a building has exceptional hazards or the fire protection equipment or system is malfunctioning or has been taken out of service. A fire watch is "the assignment of a person or persons to an area for the express purpose of notifying the fire department and/or building occupants of an emergency, preventing a fire from occurring, extinguishing small fires, or protecting the public from fire or life safety dangers."[54]

floor plate The entire floor area including the public access or common areas, tenant areas, and maintenance spaces.

floor warden Key individual on each floor of a building whose primary duty is to ensure a safe relocation or evacuation of occupants or visitors from that floor (or part thereof) during an emergency. See also *fire warden*.

incident "Event that has the capacity to lead to human, intangible or physical loss, or a disruption of an organization's operations, services, or functions — which, if not managed, can escalate into an emergency, crisis, or disaster."[55]

landlord A person or an organization that owns a facility and leases or rents it, or a part of it, to a tenant(s).

landslide "The movement of rocks, debris or earth flowing down a slope."[56]

lessee "The tenant in a lease."[57] See also *tenant*.

mobility impaired "People with physical disabilities rely on a variety of artificial means for mobility. Such devices range from canes and walkers to motorized wheelchairs."[58]

mutual aid agreement "A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement."[59]

office building A "structure designed for the conduct of business, generally divided into individual offices and offering space for rent or lease."[60]

panic "A sudden terror often inspired by a trifling cause or a misapprehension of danger and accompanied by unreasoning or frantic efforts to secure safety."[61]

partial evacuation "Immediate, general evacuation of the areas of the building nearest the fire incident. A partial evacuation may be appropriate when the building fire protection features assure that occupants away from the evacuation zone will be protected from the effects of the fire for a reasonable time. However, evacuation of additional zones may be necessary."[62] Also known as *zoned evacuation* or *staged evacuation*.

phased evacuation This strategy "provides for immediate, general evacuation of the areas of the building nearest the fire incident with continuing, selective evacuation of all other building areas.… Phased evacuation is total evacuation but not all at once."[63]

plan "A scheme or method of acting or proceeding developed in advance."[64]

portable controlled descent device See *stair descent device*.

rent "Payment for the use of space or personal property owned by another. In real estate, a fixed periodic payment by a tenant to an owner for the exclusive possession and use of leased property."[65]

runners/messengers Persons who provide physical liaison in the areas normally covered by the telephone monitors when there is a failure of telephone communications.

safe refuge area A designated area of safety for occupants inside or outside of a building. Also known as an *area of refuge* and an *area of rescue assistance*.

search monitor A person who systematically and thoroughly searches all assigned floor areas in a building to ensure that all occupants leave during an emergency evacuation.

self-evacuation "Occupants evacuating by themselves, before emergency responders have arrived on site, using available means of evacuation, i.e., elevators and stairs."[66]

shelter-in-place See *defend-in-place*.

situation awareness "The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."[67]

solicitor A person who approaches building occupants with the intent to sell something, to ask for business for a company, to request charitable contributions, or to obtain magazine subscriptions. This definition would include people who beg or panhandle for money or food.

stack effect "Results from the temperature differences between two areas, usually the inside and outside temperatures, which create a pressure difference that results in natural air movements within a building. In a high-rise building, this effect is increased due to the height of the building. Many high-rise buildings have a significant stack effect, capable of moving large volumes of heat and smoke through the building."[68]

staged evacuation See *partial evacuation* or *zoned evacuation*.

stair descent device Used during emergencies to assist physically impaired persons to travel down building stairs. Such equipment includes stairway evacuation chairs and portable controlled descent devices. The latter are not to be confused with various types of harnesses, chutes, and platforms designed to evacuate occupants down the outside of a building.[69]

stairwell monitor A person who lines up occupants in an orderly fashion at the entrance to the stairwell, organizes an orderly flow of persons into the stairwell when evacuation begins, and closes the stairwell door when no one is moving through it.

suite warden A key individual of an office suite whose primary duty is to ensure a safe relocation or evacuation of occupants or visitors from the suite during an emergency.

tabletop exercise "A test method that presents a limited simulation of an emergency or crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation."[70]

telephone monitor A person who provides telephone liaison between the floor warden and floor response personnel, liaison between the floor warden and the fire safety director or the fire department, and liaison between floors.

tenant A person, a group of persons, or a company or firm that rents or owns, and occupies space within a building. "A legal term for one who pays rent to occupy or gain possession of real estate; the lessee in a lease. Real estate managers often limit the use of the term tenant to commercial tenants and refer to residential tenants as residents."[71] See also *lessee*.

tenant information manual See *tenant manual*.

tenant manual "A compilation of management policies and procedures that relate to commercial tenants and the use of their leased space."[72] See also *tenant information manual*.

testing "A set of problems, questions, for evaluating abilities, aptitudes, skills, or performance. The means by which the presence, quality, or genuineness of anything is determined."[73]

total evacuation This strategy involves the simultaneous evacuation of all building occupants to an outside area of refuge or safety.

train "To give the discipline and instruction, drill, practice, designed to impart proficiency or efficiency."[74]

visitor In office buildings, it is a non-occupant who spends time at the building. In hotel buildings, it is a non-guest who visits a hotel guest or uses its facilities (such as meeting rooms, conference facilities, recreational facilities, restaurants, bars, a casino, or a discotheque). In residential and apartment buildings, it is a "nonresident who spends time at the home of a resident (with that resident's consent) but does not stay overnight."[75] In a mixed-use building, it could be all the preceding depending on the nature of its occupancies.

zoned evacuation "Immediate, general evacuation of the areas of the building nearest the fire incident. A partial evacuation may be appropriate when the building fire protection features assure that occupants away from the evacuation zone will be protected from the effects of the fire for a reasonable time. However, evacuation of additional zones may be necessary."[76] Also known as *partial evacuation* or *staged evacuation*.

ADDITIONAL READING

[1] American National Standards Institute (ANSI) American National Standard — ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use. Alexandria, VA: ASIS International; March 12, 2009.

[2] Are Your Tenants Safe? BOMA's Guide to Security and Emergency Planning. Washington, DC: BOMA International; 2000. Building Owners and Managers Association.

[3] ASIS Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery. Alexandria, VA: ASIS International; January 2005.

[4] ASIS International Commercial Real Estate Council Web site, <www.asisonline.org/councils/CRE.xml>.

[5] Azano HJ. CPP, CFE. Fire safety and security for high-rise buildings. Crete, IL: Abbott Langer & Associates; 1995.

[6] Emergency Preparedness. Washington, DC: BOMA International; 2002.

[7] Fire protection handbook. Quincy, MA: National Fire Protection Association; 2008. Addresses various occupancies including office buildings.

[8] Kitteringham G. CPP. Security and life safety for the commercial high-rise. Alexandria, VA: ASIS International; 2004.

[9] Nadel B. Building security handbook for architectural planning and design. New York: FAIA, McGraw Hill; 2004.

[10] NFPA 1600: Standard on disaster/emergency management and business continuity programs. Quincy, MA: NFPA International; 2007.

[11] Siegel M. Societal security management system standards: security management system consultant. : ASIS International; 2008. <www.asisonline.org/guidelines/Societal-Security-Management-System-Standards.pdf>; September 8, 2008.

REFERENCES

[1] Fennelly L. Glossary of real estate management terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003. p. 120.

[2] Bell JR. Hotels Fire protection handbook, 18th ed. Quincy, MA: National Fire Protection Association; 1997. p. 9–64.

[3] Introduction. In: Commercial building security: The notebook lesson series for security officers. Oakland, CA: American Protective Services, Inc.; 1980. p. 3.

[4] FEMA 426: Reference manual to mitigate potential terrorist attacks against buildings. Washington DC: FEMA Risk Management Series; 2003. p. 1–5.

[5] Dates and some details of bombing incidents involving Al Qaeda versus United States and Allies, 1995–2003, was obtained from The Chicago Project on Suicide Terrorism, Robert Pape, Professor of Political Science, The University of Chicago, http://jtac.uchicago.edu/conferences/05/resources/pape_formatted%20for%20DTRA.pdf; May 17, 2008. Fire dates checked against Key dates in fire history, NFPA Web site, www.nfpa.org/itemDetail.asp?categoryID51352&itemID530955&URL5Research%20&%20Reports/Fire%20statistics/Key%20dates%20in%20fire%20history; May 17, 2008. The International listing of fatal high-rise structure fires: 1911–present. NFPA ready reference: Fire safety in high-rise buildings. Quincy, MA: NFPA International; 2003. p. 101–113. Other information was obtained from various agencies and news sources, many of which are identified in the summaries of a number of the incidents in Chapter 3. However, at times, reports of casualties were conflicting. Therefore, the number of persons killed and injured could not always be definitively determined.

[6] Hall Jr JR. High-rise building fires. Quincy, MA: National Fire Protection Association; August 2005. p. 3.

[7] Hall JR. U.S. high-rise fires: the big picture. NFPA Journal. Quincy, MA: National Fire Protection Association; March/April 1994. p. 50.

[8] Hall JR. U.S. high-rise fires: the big picture. NFPA Journal. Quincy, MA: National Fire Protection Association; March/April 1994. p. 53.

[9] 2002 is the most recent year for which data were available for this report.

[10] Hall JR. U.S. high-rise fires: the big picture. NFPA Journal. Quincy, MA: National Fire Protection Association; March/April 1994. p. 3.

[11] Hall JR. U.S. high-rise fires: the big picture. NFPA Journal. Quincy, MA: National Fire Protection Association; March/April 1994.

[12] Hall JR. U.S. high-rise fires: the big picture. NFPA Journal. Quincy, MA: National Fire Protection Association; March/April 1994. p. 4.

[13] Hall JR. U.S. high-rise fires: the big picture. NFPA Journal. Quincy, MA: National Fire Protection Association; March/April 1994. p. 3.

[14] Hall JR. U.S. high-rise fires: the big picture. NFPA Journal. Quincy, MA: National Fire Protection Association; March/April 1994. p. 4.

[15] Adapted from FEMA 452: Risk assessment: A how-to guide to mitigate potential terrorist attacks against buildings. Washington DC: FEMA Risk Management Series; January 2005. p. 3-1.

[16] FEMA 452: Risk assessment: A how-to guide to mitigate potential terrorist attacks against buildings. Washington DC: FEMA Risk Management Series; January 2005. p. iii.

[17] Atlas RI. 21st century security and CPTED designing for critical infrastructure protection and crime prevention. Boca Raton, FL: CRC Press, Auerbach Publications, Taylor & Francis Group, LLC; 2008. p. 3.

[18] Hall JR Jr. High-rise building fires. Quincy, MA: National Fire Protection Association; August 2005. p. 19.

[19] Objectives of a security program. In: High-rise security training course. Oakland, CA: American Protective Services; 1990. p. 17.

[20] Office buildings. In: NFPA 730: Guide to premises security. Quincy, MA: NFPA International; 2008. p. 41.

[21] Geiger G, Craighead G. Minding the store: office security is big business. Los Angeles Business Journal July 1991:11B.

[22] Commercial building security: The notebook lesson series for security officers. Oakland, CA: American Protective Services; 1980. p. 11.

[23] Adapted from Commercial building security: The notebook lesson series for security officers. Oakland, CA: American Protective Services; 1998. p. 47.

[24] Macklowe H. Comments in the glass shield. Access Control & Security Systems Magazine February 1998. p. 21–2.

[25] Finneran ED. Security supervision: A handbook for supervisors and managers. Stoneham, MA: Butterworth-Heinemann; 1981, as reported in Fennelly LJ. Handbook of loss prevention and crime prevention. 4th ed. Burlington, MA: Elsevier Butterworth-Heinemann; 2004. p. 194.

[26] Vitch ML, Nason R. High-rise security issues. Cumming, GA: Security Technology & Design; August 1995. p. 62.

[27] NFPA. Glossary of terms, national fire code. Quincy, MA: National Fire Protection Association; 2005.

[28] Oliver E, Wilson J. Practical security in commerce and industry, 3rd ed. UK: Gower Press; 1978. p. 69.

[29] Dobbie T. Patrol techniques In: Protection officer training manual, 5th ed. International Foundation for Protection Officers, Calgary, Alberta, Canada: Butterworth-Heinemann; 1992. p. 3.

[30] Roughton J. Scanning the lines for security. Security management. Alexandria, VA: ASIS International; January 1989. p. 52

[31] American National standards Institute (ANSI) American National Standard — ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use. Alexandria, VA: ASIS International; March 12, 2009. p. 47.

[32] American National standards Institute (ANSI) American National Standard — ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use. Alexandria, VA: ASIS International; March 12, 2009. p. 46.

[33] Koob P. Australian emergency management glossary. Australian Emergency Manuals Series, Part I, The Fundamentals, Manual 3, Emergency Management Australia Canberra; 1998, as quoted in the SRM Lexicon, SRMBOK Security Risk Management Body of Knowledge, Julian Talbot and Dr. Miles Jakeman. Carlton South, Vic: Risk Management Institution of Australasia Limited; 2008. p. 346.

[34] American National standards Institute (ANSI) American National Standard — ASIS SPC.1-2009, Organizational Resilience. Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use. Alexandria, VA: ASIS International; March 12, 2009. p. 45.

[35] *Webster's College Dictionary*. 1992 edition. From *Webster's College Dictionary* by Random House, Inc. Copyright 1995, 1992, 1991. Reprinted by permission of Random House, Inc.; New York, 1992.

[36] A term obtained by combining the definition of emergency management by Koob P. Australian emergency management glossary. Australian Emergency Manuals Series, Part I, The Fundamentals, Manual 3, Emergency Management Australia Canberra; 1998, as quoted in the SRM Lexicon, SRMBOK Security Risk Management Body of Knowledge, Julian Talbot and Dr. Miles Jakeman (Carlton South, Vic: Risk Management Institution of Australasia Limited; 2008. p. 346) and the definition of a plan from *Webster's College Dictionary*, 1992 edition (from *Webster's College Dictionary*, by Random House Inc. Copyright 1995, 1992, 1991. Reprinted by permission of Random House, Inc., New York; 1992).

[37] Disaster control. Protection of assets manual. Vol. 1. Original copyright Los Angeles, CA: The Merritt Company, POA Publishing; 1991, p. 10–13.

[38] Endsley MR. Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors Society 32nd Annual Meeting. Santa Monica, CA: Human Factors Society; 1988. p. 97–101 as reported in "Achieving situation awareness is the primary challenge to optimizing building movement strategies" prepared for the NIST Workshop on Building Occupant Movement during Fire Emergencies, by Groner NE. John Jay College of Criminal Justice. City University of New York; June 9–10, 2004.

[39] Definition by Americans with Disabilities (ADA) as quoted by Cummings RB, Jaeger T. TW in ADA sets a new standard for accessibility. NFPA journal. Quincy, MA: National Fire Protection Association; May/June 1993. p. 46.

[40] Business Continuity Planning. Wikipedia, http://en.wikipedia.org/wiki/Business_continuity_planning; July 9, 2008.

[41] American National standards Institute (ANSI) American National Standard — ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use. Alexandria, VA: ASIS International; March 12, 2009. p. 45.

[42] O'Connor DJ, Cohen B. Strategies for occupant evacuation during emergencies Fire protection handbook, 20th ed. Quincy, MA: National Fire Protection Association; 2008. p. 4–105.

[43] O'Connor DJ, Cohen B. Strategies for occupant evacuation during emergencies In: Fire protection handbook, 20th ed. Quincy, MA: National Fire Protection Association; 2008. p. 4–105.

[44] Americans with Disabilities Act (ADA), Title 42, U.S. Code, Chapter 126, Section 12102.

[45] Fire risks for the mobility impaired. Emmitsburg, MD: U.S. Fire Administration, www.usfa.fema.gov; FA-204/December 1999. p. 8.

[46] American National Standards Institute (ANSI) American National Standard — ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use. Alexander, VA: ASIS International; March 12, 2009. p. 46.

[47] NFPA. Glossary of terms, national fire code. Quincy, MA: National Fire Protection Association; 2005.

[48] Wikipedia, http://en.wikipedia.org/wiki/Dumpster_%28term%29; July 19, 2008.

[49] Koob P. Australian emergency management glossary. Australian Emergency Manuals Series, Part I, The Fundamentals, Manual 3, Emergency Management Australia Canberra 1998, as quoted in the SRM Lexicon, srmbok Security Risk Management Body of Knowledge, Julian Talbot and Dr. Miles Jakeman. Carlton South, Vic: Risk Management Institution of Australasia Limited; 2008. p. 346.

[50] NFPA. Glossary of terms, national fire code. Quincy, MA: National Fire Protection Association; 2005.

[51] United Nations International Strategy for Disaster Reduction. Terminology: Basic terms of disaster risk reduction, www.unisdr.org/eng/library/lib-terminology-eng%20home.htm 31March 2004; July 8, 2008. The combined definition stated here uses a slightly modified version of the United Nations terminology. The UN definition states that emergency management is "the organization and management of resources and responsibilities for dealing with all aspects of emergencies, in particular preparedness, response and rehabilitation." The word rehabilitation has been removed. The reason for this is that for the purposes of this book, an emergency management plan addresses preparedness and response to an emergency and shortly thereafter. It does not deal with the rehabilitation process because, in the opinion of the author, that process is part of business continuity planning, which is "an interdisciplinary concept used to create and validate a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption." Business Continuity Planning. Wikipedia, http://en.wikipedia.org/wiki/Business_continuity_planning; July 9, 2008.

[52] The term is obtained by combining the definition of emergency management by Koob P. Australian emergency management glossary. Australian Emergency Manuals Series, Part I, The Fundamentals, Manual 3, Emergency Management Australia Canberra 1998, as quoted in the SRM Lexicon, srmbok Security Risk Management Body of Knowledge, Julian Talbot and Dr. Miles Jakeman (Carlton South, Vic: Risk Management Institution of Australasia Limited; 2008. p. 346) and the definition of a plan from *Webster's College Dictionary*. 1992 edition. (From *Webster's College Dictionary* by Random House, Inc. Copyright 1995, 1992, 1991. Reprinted by permission of Random House, Inc, New York; 1992.)

[53] Emergency Operations Centers. DavisLogic Inc. October 30, 2005, www.davislogic.com/EOC.htm; October 29, 2008.

[54] NFPA. Glossary of terms, national fire code. Quincy, MA: National Fire Protection Association; 2005.

[55] American National standards Institute (ANSI) American National Standard — ASIS SPC.1-2009, Organizational Resilience: Security, Preparedness, and Continuity Management Systems — Requirements with Guidance for Use. Alexandria, VA: ASIS International; March 12, 2009. p. 47.

[56] Cruden (1991) as quoted in Paper 10: Landslides in the Hillside development in the Hulu Kland, Klang Valley by Farisham Abu Samah, p. 150, http://eprints.utm.my/1627/1/LANDSLIDES_IN_THE_HILLSIDE_DEVELOPMENT___IN_THE_HULU_KLANG,_KLANG_VALLEY.pdf; August 23, 2008.

[57] Glossary of real estate management terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003. p. 94.

[58] Fire risks for the mobility impaired. Emmitsburg, MD: U.S. Fire Administration, www.usfa.fema.gov; FA-204/December 1999. p. 8.

[59] ASIS business continuity guideline. Alexandria, VA: ASIS International; January 2005. p. 8.

[60] Glossary of real estate management terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003. p. 120.

[61] Webster's third new international dictionary. Springfield, MA: Merriam-Webster; 1993.

[62] O'Connor DJ, Cohen B. Strategies for occupant evacuation during emergencies Fire protection handbook, 20th ed. Quincy, MA: National Fire Protection Association; 2008. p. 4–104.

[63] O'Connor DJ, Cohen B. Strategies for occupant evacuation during emergencies Fire protection handbook, 20th ed. Quincy, MA: National Fire Protection Association; 2008. p. 4–105.

[64] *Webster's College Dictionary*, 1992 edition. From Webster's College Dictionary by Random House, Inc. Copyright 1995, 1992, 1991. Reprinted by permission of Random House, Inc., New York; 1992.

[65] Glossary of real estate management terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003. p. 146.

[66] Emergency evacuation elevator systems guideline. Chicago, IL: Council on Tall Buildings and Urban Habitat; 2004. p. 46.

[67] Endsley MR. Design and evaluation for situation awareness enhancement. In: Proceedings of the Human Factors Society 32nd Annual Meeting. Santa Monica, CA: Human Factors Society; 1988. p. 97–101, as reported in "Achieving situation awareness is the primary challenge to optimizing building movement strategies" prepared for the NIST Workshop on Building Occupant Movement during Fire Emergencies, June 9–10, 2004, by Groner NE. John Jay College of Criminal Justice, City University of New York; June 9–10, 2004.

[68] Quiter JR. High-rise buildings Fire protection handbook, 20th ed. Quincy, MA: National Fire Protection Association; 2008. p. 20–80.

[69] Emergency procedures for employees with disabilities in office buildings. Federal Emergency Management Agency, United States Fire Administration. Emmitsburg, MD, www.usfa.dhs.gov/downloads/pdf/publications/fa-154.pdf; December 22, 2008. A reference for such information.

[70] Business continuity guideline: A practical approach for emergency preparedness, crisis management, and disaster recovery. Alexandria, VA: ASIS International; 2004. p. 10.

[71] Glossary of real estate management terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003. p. 171.

[72] Glossary of real estate management terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003. p. 171.

[73] Webster's College Dictionary, 1992 edition. From Webster's College Dictionary by Random House, Inc. Copyright 1995, 1992, 1991. Reprinted by permission of Random House, Inc., New York; 1992.

[74] Webster's College Dictionary, 1992 edition. From Webster's College Dictionary by Random House, Inc. Copyright 1995, 1992, 1991. Reprinted by permission of Random House, Inc., New York; 1992.

[75] Glossary of real estate management terms. Chicago, IL: Institute of Real Estate Management of the National Association of Realtors; 2003. p. 182.

[76] O'Connor DJ, Cohen B. Strategies for occupant evacuation during emergencies Fire protection handbook, 20th ed. Quincy, MA: National Fire Protection Association; 2008. p. 4–104.